ACTA MATHEMATICA

ACADEMIAE SCIENTIARUM HUNGARICAE

ADIUVANTIBUS

G. ALEXITS, E. EGERVÁRY, L. FEJÉR, CH. JORDÁN,
L. KALMÁR, L. RÉDEI, A. RÉNYI, F. RIESZ,
B. SZ.-NAGY, GY. SZ.-NAGY, P. TURÁN, O. VARGA

REDIGIT

G. HAJÓS

TOMUS IV.

AKADÉMIAI KIADÓ, BUDAPEST
1953

ACTA MATHEMATICA

ACADEMIAE SCIENTIARUM HUNGARICAE

A MAGYAR TUDOMÁNYOS AKADÉMIA III. OSZTÁLYÁNAK
MATEMATIKAI KÖZLEMÉNYEI

SZERKESZTŐSÉG ÉS KIADÓHIVATAL: BUDAPEST, V., ALKOTMÁNY U. 21

*

Az Acta Mathematica német, angol, francia és orosz nyelven közöl értekezéseket a matematika köréből.

Az Acta Mathematica változó terjedelmű füzetekben jelenik meg, több füzet alkot egy kötetet.

A közlésre szánt kéziratok a következő címre küldendők:

Acta Mathematica, Budapest 502, Postafiók 24.

Ugyanerre a címre küldendő minden szerkesztőségi és kiadóhivatali levelezés.

Az Acta Mathematica előfizetési ára kötetenként belföldre 80 forint, külföldre 110 forint. Megrendelhető a belföld számára az „Akadémiai Kiadó"-nál (Budapest, V., Alkotmány utca 21. Bankszámla 05-915-111-46), a külföld számára pedig a „Kultúra" Könyv- és Hírlap Külkereskedelmi Vállalatnál (Budapest, I., Fő utca 32. Bankszámla 43-790-057-181) vagy annak külföldi képviseleteinél és bizományosainál.

Die Acta Mathematica veröffentlichen Abhandlungen aus dem Bereiche der mathematischen Wissenschaften in deutscher, englischer, französischer und russischer Sprache.

Die Acta Mathematica erscheinen in Heften wechselnden Umfanges. Mehrere Hefte bilden einen Band.

Die zur Veröffentlichung bestimmten Manuskripte sind an folgende Adresse zu senden

Acta Mathematica, Budapest 502, Postafiók 24.

An die gleiche Anschrift ist auch jede für die Redaktion und den Verlag bestimmte Korrespondenz zu richten.

Abonnementspreis pro Band: 110 Forints. Bestellbar bei dem Buch- und Zeitungs-Außenhandels-Unternehmen „*Kultura*" (Budapest, I., Fő utca 32. Bankkonto Nr. 43-790-057-181) oder bei seinen Auslandvertretungen und Kommissionären.

BEDINGTES ARTINSCHES SYMBOL MIT ANWENDUNG IN DER KLASSENKÖRPERTHEORIE

Von

LADISLAUS RÉDEI (Szeged), korrespondierendem Mitglied der Akademie

Durchgängige Bezeichnungen:

$O(\ldots)$ die Anzahl der Elemente einer endlichen Menge, insbesondere die Ordnung einer endlichen Gruppe.

$g(\ldots)$ der Grad eines Relativkörpers (von endlichem Grade).[1]

$\mathfrak{G}(\ldots)$ die Galoissche Gruppe eines Galoisschen Relativkörpers.

$\{\ldots\}$ die durch die eingeklammerten Elemente erzeugte Gruppe.

n beliebige natürliche Zahl.

l eine feste positive Primzahl.

Ω ein absolut algebraischer Zahlkörper endlichen Grades.

H eine Weber—Takagische Idealgruppe in Ω,[2] von der wir ohne wesentliche Einschränkung der Allgemeinheit annehmen dürfen, daß die (zugehörige) Klassenzahl eine Potenz (>1) von l ist.[3]

$\mathfrak{H}$ die Klassengruppe von Ω mit der Hauptklasse H. Man pflegt $\mathfrak{H}$ eine l-Klassengruppe zu nennen.

e_n die Anzahl der durch l^n teilbaren Invarianten von $\mathfrak{H}$.

l^ν das Maximum der Invarianten von $\mathfrak{H}$ (d. h. $e_1 \geqq \ldots \geqq e_\nu > > e_{\nu+1} = e_{\nu+2} = \ldots = 0$).

$C, C', \ldots$ irgendwelche Klassen, d. h. Elemente von $\mathfrak{H}$.

$A, A', \ldots$ solche Klassen, für die $A^l = A'^l = \ldots = H$ gilt (das sind H und die Klassen l-ter Ordnung).

[1] Ein Relativkörper wird üblicherweise mit $\ldots|\ldots$ bezeichnet, wo links und rechts der Oberkörper bzw. Grundkörper zu stehen hat. Bezüglich Relativkörper sagen wir oft „Grad" statt „Relativgrad" usw.

[2] Bezüglich der Grundbegriffe und Hauptsätze der Klassenkörpertheorie, sowie der in dieser üblichen Terminologie und Bezeichnungsart verweise ich ein für allemal auf die Arbeiten von HASSE [1]. (Mit [ ] verweisen wir auf das Literaturverzeichnis am Schluß unserer Arbeit.)

[3] Ω und H bleiben für die ganze Arbeit als festgewählt betrachtet, alle übrigen Begriffe, die oben noch folgen, sind aus diesen zwei Angaben Ω, H abgeleitet. Wenn nichts anderes gesagt wird, so spielt Ω die Rolle eines „Grundkörpers".

$\mathfrak{A}_n$ die Gruppe derjenigen A, die von der Form $C^{l^{n-1}}$ (d. h. l^{n-1}-te Potenzen) sind.[4]

Ω_H der H zugeordnete Klassenkörper von Ω. Die Unterkörper von $\Omega_H|\Omega$ nennen wir kurz Klassenkörper, insbesondere Ω_H den vollen Klassenkörper.

$\mathsf{K}, \mathsf{K}', \ldots$ Klassenkörper vom Grade l über Ω.

$\mathsf{K}_n, \mathsf{K}_n', \ldots$ relativzyklische Klassenkörper vom Grade l^n über Ω. (Diese existieren nur für $n \leqq \nu$.) Insbesondere bedeuten also $\mathsf{K}_1, \mathsf{K}_1', \ldots$ dasselbe wie $\mathsf{K}, \mathsf{K}', \ldots$ Man setze noch bequemlichkeitshalber $\mathsf{K}_0 = \mathsf{K}_0' = \ldots = \Omega$.

$\mathfrak{M}_n$ die Menge derjenigen K, über denen es mindestens ein K_n gibt.[5]

$\Pi_n (n \leqq \nu)$ das Produkt[6] der $\mathsf{K}(\in \mathfrak{M}_n)$.

Ω_n das Produkt der K_i $(i \leqq n)$. Wir nennen Ω_n kurz den n-ten Klassenkörper. Insbesondere ist $\Omega_H = \Omega_\nu$, $\Pi_1 = \Omega_1$. Es werde $\Omega_0 = \Omega$ gesetzt.

$\left(\frac{\Lambda}{C}\right)$ das Artinsche Symbol für beliebige Klassenkörper Λ in „invarianter Schreibweise".[7]

§ 1. Einleitung

Es ward mir klar, daß in meiner früheren Arbeit [5] eine Verallgemeinerung durchzuführen ist, um hierdurch die bequemere Anwendbarkeit zu sichern. Zum Zweck dieser Verallgemeinerung schien mir nötig, alles von Grund aus neu aufzubauen, ohne dabei die Kenntnis von [5] vorauszusetzen. (Dementsprechend werden wir hier über die auch schon in [5] eingeführten Begriffe so sprechen, als wenn sie uns erst jetzt aufgetaucht wären.) Vieles wird hier ausführlicher besprochen, auch werden teils andere Bezeichnungen und Benennungen eingeführt. Selbst die gemeinte Verallgemeinerung wird unter anderem zur Folge haben, daß man gewisse Aufklärungen über die

[4] Für $n > \nu$ ist $\mathfrak{A}_n$ die Gruppe mit dem einzigen Element H (d. h. $O(\mathfrak{A}_n) = 1$ für $n > \nu$).

[5] Für $n > \nu$ ist $\mathfrak{M}_n$ die leere Menge (d. h. $O(\mathfrak{M}_n) = 0$ für $n > \nu$).

[6] Unter dem Produkt $k_1 \ldots k_r$ von Unterkörpern eines Körpers verstehen wir den sogenannten zusammengesetzten Körper, d. h. den durch die Elemente von $k_1, \ldots, k_r$ erzeugten Unterkörper.

[7] D. h. $\left(\frac{\Lambda}{C}\right) = \left(\frac{\Lambda|\Omega}{\mathfrak{a}}\right)$ $(\mathfrak{a} \in C)$, wobei rechts die übliche Schreibweise des Artinschen Symbols steht, wofür man kürzer auch $\left(\frac{\Lambda}{\mathfrak{a}}\right)$ zu schreiben pflegt. Da $\left(\frac{\Lambda}{\mathfrak{a}}\right)$ nur von der Klasse abhängt, der $\mathfrak{a}$ angehört, so ist die invariante Schreibweise $\left(\frac{\Lambda}{C}\right)$ eindeutig und daher berechtigt.

Einheiten in Ω gewinnen kann, worüber wir näheres in der Bemerkung 2 am Schluß von § 2 sagen werden.

Ein Hauptproblem der Zahlentheorie ist, daß man von den bloßen Angaben Ω, H ausgehend die Struktur von $\mathfrak{H}$ bestimmt, womit wir die Berechnung (von ν und) der Zahlen e_n ($n=1,\ldots,\nu$) meinen. Zum großen Teil ist die Klassenkörpertheorie aus diesem Problem entsprungen; umgekehrt liefert diese die Lösung des Problems durch die Konstruktion des vollen Klassenkörpers Ω_H. Prinzipiell steht dieser Konstruktion nichts im Wege. Man kann so vorgehen, daß man Klassenkörper K_n in genügender Zahl konstruiert, aus denen sich Ω_H zusammensetzen läßt. Selbst die Konstruktion eines K_n kann so geschehen werden, daß man nach und nach die Glieder der K_n eindeutig zugehörenden Körperkette $K=K_1\subset K_2\subset\ldots,\subset K_n$ konstruiert. Dabei ist der Relativkörper $K_i|K_{i-1}$ zyklisch vom Grade l, weshalb sich K_n durch n *elementare Körperkonstruktionen* erreichen läßt. Wie einfach das auch gelautet hat, so steckt doch eine Menge Unsicherkeit dahinter, denn man kann ja Ω_H im allgemeinen auf sehr verschiedene Weise aus Körpern K_n zusammensetzen, eine Freiheit, die aber auch überflüssige Arbeit verursachen kann. Man muß sich deshalb offen eingestehen, daß man bisher über kein genügend ausgearbeitetes Verfahren zur Konstruktion von Ω_H und zur Erforschung der Struktur von $\mathfrak{H}$ auf klassenkörpertheoretischer Grundlage verfügt. Der Zweck unserer Arbeit ist unter anderem, diesem Mangel mit einem „invarianten Verfahren" abzuhelfen.

Die Führerrolle wird ein gewisses (zweiwertiges) Symbol[9]

$$\left(\frac{K}{C}\right)_n \tag{1}$$

spielen, das wir *bedingtes Artinsches Symbol* nennen.[10] Diese Benennung haben wir deshalb gewählt, da (1) begrifflich dem Artinschen Symbol nahe steht

[8] Eine Körperkonstruktion nennen wir elementar, wenn es sich um eine relativzyklische Erweiterung vom Relativgrade l handelt. Die Ausführung solcher Konstruktionen ist bekanntlich als eine allgemein erledigte Aufgabe anzusehen (ob der Ausgangskörper die l-ten Einheitswurzeln enthält oder nicht enthält).

[9] Die vollständige Bezeichnung von (1) wäre $\left(\frac{K\,|\,\Omega}{C}\right)_n$. In der Arbeit [5] haben wir (1) mit $(K, C)_n$ bezeichnet, obige Bezeichnung scheint aber vorteilhafter zu sein. Hier bemerken wir, daß wir die Benennung „bedingtes Artinsches Symbol" in der Arbeit [5] noch nicht verwendet haben. Ferner bemerken wir, daß wir in einer früheren Arbeit [4] ein Symbol $\{a, b, c\}$ eingeführt haben, das für $c\,|\,ab$ einem Spezialfall von (1) gleichkommt.

[10] Nach Frobenius nennen wir bei festem C die Menge aller Klassen C^i ($l \not| i$) eine Abteilung (von $\mathfrak{H}$). Offenbar bilden die Abteilungen eine Einteilung von $\mathfrak{H}$ in Äquivalenzklassen. Wir werden sehen (vgl. (7)), daß (1) für alle Klassen C gleich ist, die in einer Abteilung liegen. Deshalb dürfte man für (1) die „invariante Schreibweise" $\left(\frac{K}{\mathfrak{C}}\right)_n$ einführen, wobei $\mathfrak{C}$ die durch C repräsentierte Abteilung bezeichnet.

und (im Fall $n \geqq 2$) nur für gewissen Bedingungen genügende K, C existiert (s. die Definition am Anfang von § 2). Unser Hauptsatz (s. § 2) wird lehren, daß die Struktur von $\mathfrak{H}$ sich sehr übersichtlich mit Hilfe von Symbolen (1) erforschen läßt.[11] Und zwar werden sich von einer gewissen Matrix M_1 ausgehend nach einem einfachen *Algorithmus* weitere Matrizen $M_2, M_3, \ldots$ bilden lassen, wobei M_n aus Elementen $\left(\frac{\mathrm{K}}{A}\right)_n$ besteht, so daß e_n eben als die Anzahl der Spalten von M_n kenntlich wird.[12]

Nach dem Gesagten können wir in unserem Algorithmus ein vollkommenes Werkzeug zur Untersuchung von $\mathfrak{H}$ erblicken, das in theoretischer Hinsicht nichts zu wünschen übrigläßt, aber in konkreten Fällen müssen zur effektiven Ausführung des Algorithmus auch die Werte der Elemente von M_n berechnet werden; hierzu wird die Konstruktion von gewissen Klassenkörpern K_n nötig. Unser Algorithmus wird uns auch den kürzesten Weg angeben, auf dem man die nötigen Konstruktionen ausführen kann, und zwar so, daß gleichzeitig auch Ω_H entsteht, als Produkt der konstruierten Körper K_n. Dabei wird die so geschilderte Art der Konstruktion von Ω_H nach einer strengen Systematik eingerichtet, die einem jede überflüssige Mühe erspart.

Es gilt auch allgemeiner, daß wenn man in unserem Algorithmus bis zur Bestimmung der Zahlen $e_1, \ldots, e_n$ vorgedrungen ist, so liefert das Produkt der inzwischen konstruierten Körper K_i eben den $n-1$-ten Klassenkörper $\Omega_{n-1} (n = 1, \ldots, \nu + 1)$.

Die in unseren Resultaten zu erzielende Eleganz wird dem Begriff des bedingten Artinschen Symbols zuzuschreiben, weshalb sein Bürgerrecht zweifellos dasteht. Wir bemerken hierzu, daß uns zur Schaffung dieses Begriffs eine lange Reihe vorheriger Untersuchungen mit zwingender Kraft angeleitet hat (vgl. das Literaturverzeichnis am Schluß unserer Arbeit [7]), aber auch ohne uns schon hier auf diese Untersuchungen zu berufen, können wir dem Leser den Begriff des bedingten Artinschen Symbols mit einem einfachen klassischen Beispiel nahebringen. Wir meinen das rationale biquadratische Restsymbol $\left(\frac{a}{b}\right)_4$ von Dirichlet. Dieses definiert man insbesondere für positive ungerade Primzahlen $b = p \equiv 1 \pmod 4$ unter der Bedingung

$$\left(\frac{a}{p}\right) = 1,$$

[11] Genauer gesagt, werden dabei unter allen Symbolen (1) nur die $\left(\frac{\mathrm{K}}{A}\right)_n$ benützt, weshalb zu unseren Zwecken genug gewesen wäre, das bedingte Artinsche Symbol nur in diesem einfachsten Spezialfall zu definieren. Die größere Allgemeinheit wird uns keine Mühe verursachen und kann bei den Anwendungen nützlich sein.

[12] Die Folge $M_1, M_2, \ldots$ wird im wesentlichen eindeutig bestimmt sein, weshalb sie als eine Invariante von Ω und H anzusehen ist.

wobei links das Symbol von Legendre steht, und zwar versteht man dann unter dem Symbol $\left(\frac{a}{p}\right)_4$ die Zahl 1 oder -1, je nachdem a ein biquadratischer Rest mod p oder kein solcher ist. Nun gilt auch

$$\left(\frac{a}{p}\right)_4 = \left(\frac{a|R(i)}{\pi}\right)_4, \tag{2}$$

wobei R der rationale Zahlkörper, $R(i)$ der Gaußsche Zahlkörper, π eine ganze Zahl in $R(i)$ mit der Norm p ist, und rechts das 4-te Potenzrestsymbol in $R(i)$ steht. Hiernach kommt das Dirichletsche Symbol $\left(\frac{a}{p}\right)_4$ einem (gewöhnlichen!) Potenzrestsymbol in $R(i)$ gleich, *aber seine Existenz ist an die Bedingung geknüpft, daß das (einfacher gebaute) Restsymbol* $\left(\frac{a}{p}\right)$ *den Wert* 1 *hat.* Um diesem Tatbestand Ausdruck zu geben, wollen wir das Dirichletsche Symbol ein *bedingtes Potenzrestsymbol* nennen. Da das (gewöhnliche) Potenzrestsymbol seine weitstgehende Verallgemeinerung im Artinschen Symbol hat, so erblicken wir auch schon in dieser einfachen Bemerkung über (2) einen Ansatz zur Definition des bedingten Artinschen Symbols. In der Tat wird letzteres Symbol das bedingte Dirichletsche Retsymbol als Spezialfall in sich enthalten, wie wir das in der Arbeit [7] sehen werden. Aus diesen Gründen können wir sagen, daß das bedingte Artinsche Symbol eine Synthese des Dirichletschen und des Artinschen Symbols ist.[13 14]

Wir gliedern unsere Arbeit so:

Im § 2 sprechen wir von der Definition des bedingten Artinschen Symbols und seinen zwei Produktregeln ausgehend möglichst schnell unseren

[13] Das oftmalige Auftreten des Dirichletschen Symbols in sehr verschiedenen Fragen ist hinlänglich bekannt. Man weiß auch, daß (2) kein äußerer Schmuck, sondern eine wesentliche Eigenschaft dieses Symbols ist, da man oft genötig ist, $\left(\frac{a}{p}\right)_4$ durch die rechte Seite von (2) zu ersetzen. Von dem bedingten Artinschen Symbol sind ebenfalls weitere Anwendungen zu erwarten, auch auf anderen Gebieten, ferner muß man sich dazu vorbereiten, daß man während der Untersuchungen von den bedingten Artinschen Symbolen eventuell auf gewöhnliche Artinsche Symbole übergehen soll. (Solches wird bei uns im § 6 geschehen.)

[14] Insbesondere bietet (2) zur Anwendung des Reziprozitätssatzes in $R(i)$ eine Möglichkeit. So kommt man zur Reziprozitätsformel

$$\left(\frac{p}{q}\right)_4 \left(\frac{q}{p}\right)_4 = \left(\frac{\varkappa}{\pi}\right),$$

wobei p, q verschiedene positive Primzahlen $\equiv 1 \pmod 4$ sind, $\left(\frac{q}{p}\right) = 1$ ist, $\pi, \varkappa$ ganze Zahlen in $R(i)$ sind mit der Norm p bzw. q, ferner $\varkappa \equiv 1 \pmod 2$ ist, und rechts das quadratische Restsymbol in $R(i)$ steht. Diese Formel hat Verfasser mehrmals verwendet (vgl. [7]). Eine neue, interessante Anwendung findet sich bei Kuroda [3]. S. auch Rédei [6].

Hauptsatz aus, dem wir dann noch einen Zusatz und Bemerkungen folgen lassen.

Im § 3 beschreiben wir unseren Algorithmus.

Im § 4 folgt die Abfassung einiger Lemmas und weiterer Sätze, die sich mit wenig Ausnahme ebenfalls auf das bedingte Artinsche Symbol beziehen und zum Beweis des Hauptsatzes nötig werden.

Im § 5 beweisen wir die Lemmas und Sätze.

Im § 6 beschreiben wir die auf dem Hauptsatz beruhende „invariante Konstruktion" des vollen Klassenkörpers.

In der nachstehenden Arbeit [7] wenden wir unsere Resultate auf den Spezialfall der 2-Ringklassengruppe des quadratischen Zahlkörpers an, wodurch unter anderem auch ein langersehnter Abschluß der Theorie der Pellschen Gleichung entstehen wird.

§ 2. Das bedingte Artinsche Symbol. Zwei Produktregeln. Hauptsatz

Definition. Wenn K, C, n so beschaffen sind, daß über K mindestens ein K_n vorhanden (d. h. $K \in \mathfrak{M}_n$), ferner die Ordnung der Artinschen Symbole

$$\left(\frac{K_n}{C}\right) \qquad (K_n \supseteq K) \tag{3}$$

invariant und $\leqq l$ ist, so sagen wir, daß das *bedingte Artinsche Symbol*

$$\left(\frac{K}{C}\right)_n \tag{4}$$

existiert und setzen

$$\left(\frac{K}{C}\right)_n = 1 \quad \text{bzw.} \quad \left(\frac{K}{C}\right)_n = -1, \tag{5}$$

je nachdem die gesagte (gemeinsame) Ordnung 1 oder l ist. Wir nennen n den *Index* des bedingten Artinschen Symbols (4).[15] (Vgl. Satz 5 im § 4.)

Insbesondere existiert $\left(\frac{K}{C}\right)_1$ stets, da im Fall $n=1$ der Zähler von (3) nur K sein kann und die Ordnung von $\left(\frac{K}{C}\right)$ gleich 1 oder l ist.

Offenbar gilt für die Hauptklasse H

$$\left(\frac{K}{H}\right)_n = 1 \qquad (K \in \mathfrak{M}_n;\ n = 1, \ldots, \nu). \tag{6}$$

Ferner folgt aus obiger Definition und der multiplikativen Eigenschaft des Artinschen Symbols, daß mit (4) zusammen auch alle $\left(\frac{K}{C^i}\right)_n$ existieren und

[15] Da $\mathfrak{M}_n$ $(n > \nu)$ die leere Menge ist, so kommen nur die $n \leqq \nu$ als Indizes in Frage.

dann

(7) $$\left(\frac{K}{C^i}\right)_n = \left(\frac{K}{C}\right)_n \qquad (l \nmid i),$$

bzw.

(8) $$\left(\frac{K}{C^i}\right)_n = 1 \qquad (l | i)$$

ist.[16]

Es gelten die folgenden zwei Produktregeln, die wir im § 5 beweisen:

SATZ 1. (Produktregel des bedingten Artinschen Symbols nach dem Nenner.) *Existieren für gegebene* $n, K, C, C' (C \neq C')$ *mindestens zwei der* $l+1$ *bedingten Artinschen Symbole*

(9) $$\left(\frac{K}{C''}\right)_n \qquad (C'' = C, C', CC', C^2C', \ldots, C^{l-1}C'),$$

so existieren alle. Ist das der Fall, so sind sie entweder alle gleich 1 *oder ist genau eins unter ihnen gleich* 1.

SATZ 2. (Produktregel des bedingten Artinschen Symbols nach dem Zähler.) *Existieren für gegebene* $n, C, K, K' (K \neq K')$ *mindestens zwei der* $l+1$ *bedingten Artinschen Symbole*

(10) $$\left(\frac{K''}{C}\right)_n \qquad (K'' \subset KK'),$$

so existieren alle. Ist das der Fall, so sind sie entweder alle gleich 1 *oder ist genau eins unter ihnen gleich* 1.[17]

Um unseren Hauptsatz formulieren zu können, müssen wir vorerst einige einfache Begriffe einführen.

Betrachten wir bei beliebigem n endliche (rechteckige) Matrizen von der Form

---

[16] Wegen (7) tritt [10] in Kraft.

[17] Die ohnehin augenscheinliche Dualität der Sätze 1, 2 kommt noch mehr ans Licht, wenn für die bedingten Artinschen Symbole die in [10] erwähnte invariante Schreibweise $\left(\frac{K}{\mathfrak{C}}\right)_n$ gebraucht und das Produkt $\mathfrak{C}\mathfrak{C}'$ zweier verschiedener Abteilungen $\mathfrak{C}, \mathfrak{C}'$ als die Menge der (verschiedenen) Klassen

$$C^i C'^j \qquad \text{(nicht gleichzeitig } l | i, j)$$

definiert wird, wobei C, C' je eine beliebige Klasse in $\mathfrak{C}$ bzw. $\mathfrak{C}'$ bezeichnen. Dann handelt es sich nämlich in (9) und (10) in voller Symmetrie um $l+1$ Symbole von der Form

$$\left(\frac{K}{\mathfrak{C}''}\right)_n \qquad (\mathfrak{C}'' \subset \mathfrak{C}\mathfrak{C}'),$$

bzw.

$$\left(\frac{K''}{\mathfrak{C}}\right)_n \qquad (K'' \subset KK').$$

$$M=\begin{vmatrix} \left(\frac{K^{(1)}}{C^{(1)}}\right)_n & \left(\frac{K^{(2)}}{C^{(1)}}\right)_n & \cdots \\ \left(\frac{K^{(1)}}{C^{(2)}}\right)_n & \left(\frac{K^{(2)}}{C^{(2)}}\right)_n & \\ \vdots & & \end{vmatrix}, \tag{11}$$

die wir als Funktion der Variabeln

$$C^{(1)}, C^{(2)}, \ldots, \tag{12}$$

$$K^{(1)}, K^{(2)}, \ldots \tag{13}$$

auffassen; wir wollen uns nur ausbedingen, daß die Körper (13) unabhängig[18] sind und die Elemente von M existieren.[19]

Die Matrix M nennen wir *ausreduziert,* wenn sie eine Diagonalmatrix ist, d. h. die Elemente außerhalb der Diagonale gleich 1 sind, und in der Diagonale die Elemente 1 den Elementen -1 vorangehen.

Unter einer *elementaren Zeilentransformation* der Matrix (11) verstehen wir die Ersetzung einer Klasse $C^{(s)}$ durch eine Klasse $C''=(C^{(r)})^i C^{(s)}$ $(r\neq s;$ $i=1,\ldots,l-1)$. Ähnlich verstehen wir unter einer *elementaren Spaltentransformation* von (11) die Ersetzung eines Körpers $K^{(s)}$ durch einen Körper $K''\subset K^{(r)}K^{(s)}, \neq K^{(r)}$ $(r\neq s)$.[20] Beide Art dieser Transformationen nennen wir schlechthin *elementare Transformationen* der Matrix (11). Aus den Sätzen 1,2 folgt sofort die Richtigkeit der folgenden Aussage:

Die Matrix M kann man mit Hilfe elementarer Transformationen und Permutationen der Zeilen und Spalten ausreduzieren.

Nunmehr verstehen wir unter einer (ersten) *Ableitung* der Matrix M jede solche Matrix, die aus M so entsteht, daß man sie *erstens* ausreduziert, *zweitens* die zu den Diagonalelementen -1 gehörenden Zeilen und Spalten streicht, *drittens* in der übriggebliebenen Matrix den Index n der Elemente zu

[18] Nämlich „unabhängig über Ω". Im allgemeinen sagen wir, daß die Unterkörper $k_1,\ldots,k_r(\supseteq k)$ eines Körpers unabhängig über einem gemeinsamen Unterkörper k sind, wenn

$$g(k_1\ldots k_r|k)=g(k_1|k)\ldots g(k_r|k)$$

gilt. (Man pflegt hierfür auch zu sagen, daß $k_1,\ldots,k_r$ einander über k nicht reduzieren.) Wir bemerken hier, daß in der Arbeit [5] an zwei Stellen irrtümlicherweise „algebraisch unabhängig" statt „unabhängig" steht.

[19] Es ist eine beabsichtigte Asymmetrie, die auch in unseren Hauptsatz einziehen und eine wichtige Rolle spielen wird, daß wir nur von den Zählern und nicht auch von den Nennern der von uns in Betracht gezogenen Matrizen Unabhängigkeit verlangen.

[20] Bei obiger Definition der Zeilen- und Spaltentransformationen hat man zu berücksichtigen, daß sehr wohl auch $C^{(r)}=C^{(s)}$ $(r\neq s)$ sein kann, dagegen $K^{(r)}, K^{(s)}$ für $r\neq s$ verschieden sind. Die Bezeichnungen C'', K'' haben wir den Sätzen 1,2 angepaßt.

$n+1$ erhöht.[21] Wegen dieser Erhöhung der Indizes ist natürlich die Existenz der Elemente einer Ableitung, d. h. die der Ableitung, im allgemeinen fraglich. Wir sagen, daß die Matrix M *ableitbar* ist, wenn alle die eben gesagten („formalen") Ableitungen wirklich existieren. Ist die Matrix M ableitbar und sind alle Ableitungen von ihr wieder ableitbar, so nennen wir sie zweimal ableitbar. Es versteht sich jetzt schon von selbst, was wir unter einer *beliebig oft ableitbaren* Matrix M und einer *k-ten Ableitung* ($k \geqq 0$) von ihr zu verstehen haben. (Die 0-te Ableitung ist M selbst.) Wir nennen $M, M^{(1)}, \ldots$ eine Folge aufeinanderfolgender Ableitungen von M, wenn darin jedes Glied $M^{(k)}$ ($k=1, 2, \ldots$) eine Ableitung des vorangehenden Gliedes (also $M^{(k)}$ eine k-te Ableitung von M) ist.

Hauptsatz. *Man nehme ein (endliches) System $A^{(1)}, A^{(2)}, \ldots$ erzeugender Elemente der Gruppe $\mathfrak{A}_1$ aller A und eine Basis*[22] $\mathsf{K}^{(1)}, \mathsf{K}^{(2)}, \ldots$ *der Menge $\mathfrak{M}_1$ aller K. Die zugehörige Matrix*

$$M_1 = \left|\begin{matrix} \left(\dfrac{\mathsf{K}^{(1)}}{A^{(1)}}\right)_1 & \left(\dfrac{\mathsf{K}^{(2)}}{A^{(1)}}\right)_1 & \cdots \\ \left(\dfrac{\mathsf{K}^{(1)}}{A^{(2)}}\right)_1 & \left(\dfrac{\mathsf{K}^{(2)}}{A^{(2)}}\right)_1 & \\ \vdots & & \end{matrix}\right| \tag{14}$$

ist beliebig oft ableitbar und in jeder Folge

$$M_1, M_2, \ldots \tag{15}$$

ihrer aufeinanderfolgenden Ableitungen ist die Anzahl der Spalten von M_n gleich $e_n (=1, 2, \ldots)$. Insbesondere ist also ν die größte Zahl, für die M_ν nicht leer ist.

Bemerkung 1. Nach der Definition der Ableitung besteht M_n aus lauter Elementen von der Form $\left(\dfrac{\mathsf{K}}{A}\right)_n$. Mit mehr Eleganz läßt sich der Hauptsatz so aussprechen, daß man auch für $A^{(1)}, A^{(2)}, \ldots$ eine Basis[23] von $\mathfrak{A}_1$ nimmt. Dann ist für jedes n die Matrix M_n quadratisch vom Typ $e_n \times e_n$, ferner bilden

[21] Die Ableitung ist wegen der Mehrdeutigkeit des Ausreduzierens von M auch mehrdeutig. Sie kann unter Umständen auch die leere Matrix sein. Auch die Ableitung einer leeren Matrix definieren wir, und zwar verstehen wir darunter wieder die leere Matrix.

[22] Unter einer Basis der Menge $\mathfrak{M}_1$ verstehen wir jedes System von möglichst vielen unabhängigen[13] Körpern K. (Vgl. die Verallgemeinerung in[24].)

[23] Wie gewöhnt verstehen wir unter einer Basis einer endlichen Abelschen Gruppe jedes System unabhängiger erzeugender Elemente ($\neq 1$) von Primzahlpotenzordnung. (Die letzte Forderung ist von selbst erfüllt — wie auch in unserem Falle — wenn es sich um Gruppen von Primzahlpotenzordnung handelt.)

dann die Nenner und Zähler in M_n je eine Basis[24] der Gruppe $\mathfrak{A}_n$ bzw. der Menge $\mathfrak{M}_n$, was aus dem Beweis im § 5 klar wird (vgl. hierzu Lemma 1 und den Schluß von Lemma 3 im § 4). Es folgt, daß dann die Matrizenfolge (15) bis auf Zeilen- und Spaltenpermutationen und elementare Transformationen der Glieder eindeutig bestimmt, also in diesem Sinne invariant ist. Hiernach liefert der Hauptsatz, wie schon gesagt, ein invariantes Verfahren zur Erforschung der Struktur der Klassengruppe $\mathfrak{H}$. *Der allgemeine Fall,* wo man nämlich für die Nenner in M_1 beliebige Erzeugende $A^{(1)}, \ldots, A^{(t)}$ von $\mathfrak{A}_1$ nimmt ($t \geqq e_1$), unterscheidet sich vom vorigen natürlich nur wenig, trotzdem ist diese, in dem Hauptsatz steckende größere Allgemeinheit sehr wichtig. Vor allem bemerken wir, daß dann M_n ($n = 1, \ldots, \nu$) offenbar vom Typ $(e_n + t - e_1) \times e_n$ ist, ferner bilden die Nenner und Zähler in M_n immer noch ein System $e_n + t - e_1$ erzeugender Elemente von $\mathfrak{A}_n$ bzw. unverändert eine Basis von $\mathfrak{M}_n$, was aus dem Beweis im § 5 ebenfalls klar wird.

Zusatz. *Nimmt man im Hauptsatz eine Matrix M_1 vom Typ $t \times e_1$ an* ($t \geqq e_1$) *und reduziert die Matrix M_ν in* (15) *aus, so werden die Nenner in den letzten $t - e_1$ Zeilen alle gleich der Hauptklasse H.*

Bemerkung 2. Die Bedeutung des Zusatzes besteht in folgendem. Es werde angenommen, daß man irgendwie eine endliche Gruppe $\mathfrak{S}$ bestimmt hat, für die eine Homomorphie

$$\mathfrak{S} \sim \mathfrak{A}_1 \tag{16}$$

gilt, und man eine homomorphe Abbildung $\mathfrak{s} \to A(\mathfrak{s})$ von $\mathfrak{S}$ auf $\mathfrak{A}_1$ kennt ($\mathfrak{s} \in \mathfrak{S}$, $A(\mathfrak{s}) \in \mathfrak{A}_1$), endlich auch eine Basis $\mathfrak{s}^{(1)}, \ldots, \mathfrak{s}^{(t)}$ von $\mathfrak{S}$ bestimmt hat. (Diese Voraussetzungen können in der Praxis oft in sehr natürlicher Weise in Erfüllung gehen.) Wir wollen $\mathfrak{S}$ *eine abundante Erzeugung* von $\mathfrak{A}_1$ nennen, womit wir darauf hinspielen, daß die Klassen A im allgemeinen mehrfach in der Form $A(\mathfrak{s})$ ($\mathfrak{s} \in \mathfrak{S}$) erzeugt werden. Offenbar wird $\mathfrak{A}_1$ durch die Klassen

$$A(\mathfrak{s}^{(1)}), \ldots, A(\mathfrak{s}^{(t)})$$

erzeugt, die man also als Nenner zur Bildung von M_1 in (14) verwenden kann. Die Berechnung der Ableitungsfolge (15) kann dann so geschehen, daß überall, wo Satz 1 zur Anwendung kommt, das Produkt zweier Klassen nach der aus (16) folgenden Regel

$$A(\mathfrak{s})A(\mathfrak{t}) = A(\mathfrak{s}\mathfrak{t}) \qquad (\mathfrak{s}, \mathfrak{t} \in \mathfrak{S}),$$

also im wesentlichen *innerhalb der Gruppe* $\mathfrak{S}$ berechnet wird. Der Zusatz führt auf diesem Wege zu der Aussage, daß für gewisse Gruppenelemente

$$\mathfrak{t}^{(i)} \qquad (i = 1, \ldots, t - e_1),$$

[24] Ganz allgemein verstehen wir unter einer Basis einer Menge von (relativ) Abelschen Körpern $k_1|k, \ldots, k_r|k$ von endlichem Grade jedes System von Unterkörpern $k', k'', \ldots$ von $k_1 \ldots k_r|k$, wofür $k'k'' \ldots = k_1 \ldots k_r$ gilt, ferner $k', k'', \ldots$ unabhängig und vom Primzahlpotenzgrad über k sind. (Die $k_1, \ldots, k_r$ sollen dabei Unterkörper eines festen Körpers sein.)

durch die nämlich nach dem Ausreduzieren von M_ν die Nenner in den letzten $t-e_1$ Zeilen in der Form

$$A(\mathfrak{T}^{(i)}) \qquad (i=1,\ldots,t-e_1)$$

ausgedrückt werden, *diese Klassen gleich der Hauptklasse H sind.* Die wichtige Bedeutung dieser Aussage und hierdurch selbst des Zusatzes wird uns erst aus der anschließenden Arbeit [7] klar, wo wir den Hauptsatz auf die 2-Ringklassengruppe des quadratischen Zahlkörpers mit Hilfe einer abundanten Erzeugung $\mathfrak{S}$ von $\mathfrak{A}_1$ anwenden und auf diesem Wege unter anderem genaue Antwort auf das Problem des Vorzeichens der Norm der Ringeinheiten des Körpers (d. h. der Lösbarkeit der Pellschen Gleichung $x^2-dm^2y^2=-1$) gewinnen werden. (Vgl. den Schluß von § 1.) Entsprechendes ist auch in anderen Fällen mit Recht zu erwarten, daß man nämlich durch den Hauptsatz und Zusatz auch Aufklärungen über die in H liegenden Einheiten von Ω gewinnt, vorausgesetzt, daß man es mit einer abundanten Erzeugung von $\mathfrak{A}_1$ zu tun hat. Hierin liegt die eigentliche Bedeutung der am Anfang erwähnten Erweiterung unserer Untersuchungen gegenüber denjenigen in unserer früheren Arbeit [5], wo nämlich der Hauptsatz (ohne den Zusatz) enger, nämlich nur für solche Matrizen M_1 in (14) bewiesen wurde, in denen $A^{(1)}, A^{(2)},\ldots$ eine Basis von $\mathfrak{A}_1$ ist. Diese frühere engere Fassung hat für die Anwendungen eine unangenehme Schwerfälligkeit verursacht. (Ein anderer „Zusatz" fand sich auch in [5], der mit obigem nichts zu tun hat und hier mit passenden Änderungen in § 6 eingearbeitet wird.)

§ 3. Algorithmus zur Erforschung der Klassengruppe

Die im § 2 beschriebene Aufstellung einer Folge $M_1, M_2,\ldots$ in (15) nennen wir den *Algorithmus* zur Erforschung der Struktur der Klassengruppe $\mathfrak{H}$. Da nach dem Hauptsatz mit ihm der Reihe nach die Zahlen $e_1 \geqq \cdots e_\nu > e_{\nu+1}=0$ bestimmt werden. so teilen wir ihn entsprechend in $\nu+1$ „Schritte" ein, die wir der Reihe nach für $n=1,\ldots,\nu+1$ den *e_n-Schritt* des Algorithmus nennen werden. Wir wollen diese Einteilung so machen, daß allgemein die Ausführung des e_n-Schrittes zur Bestimmung von e_n eben ausreicht.

Zu diesem Zweck nennen wir eine Matrix M_n in (15) *nach den Zeilen reduziert,* wenn diese von der Form

$$\left(\begin{array}{c|c} \begin{matrix}1 & & \\ & \ddots & \\ & & 1\end{matrix} & \\ \hline (\pm 1) & \begin{matrix}-1 & & \\ & \ddots & \\ & & -1\end{matrix} \\ \hline & \end{array}\right)$$

ist, wobei die Teilmatrix (± 1) aus Elementen ± 1 besteht, und an den leeren Stellen lauter Elemente 1 stehen. (Es wurde berücksichtigt, daß M_n mindestens so viel Zeilen wie Spalten hat.) Das Ausreduzieren einer Matrix M_n kann man immer in zwei Teilen ausführen, so nämlich, daß man sie zuerst mit Zeilen- und Spaltenpermutationen und Anwendung von Satz 1 nach den Zeilen reduziert, dann mit Anwendung von Satz 2 ausreduziert. Wir bemerken, daß dieser „zweite Teil" des Ausreduzierens an der Anzahl der Diagonalelemente 1 offenbar nicht mehr ändert. Wegen des Hauptsatzes folgt hieraus, daß es zur Berechnung von e_n ($n \geqq 2$) genügt, die Matrix M_{n-1} in (15) nach den Zeilen zu reduzieren (statt ihre Ableitung M_n zu bilden), und zwar wird $e_n = e_{n-1} - r_n$, wobei r_n die Anzahl der Elemente -1 bezeichnet, die in der Diagonale von M_{n-1} auftreten, wenn diese nach den Zeilen reduziert wird. (Also ist r_n eine Invariante der Matrizen M_{n-1}.) Nach allem diesen definieren wir die e_n-Schritte endgültig wie folgt.

Der e_1-Schritt soll in der Aufstellung einer Basis $K^{(1)}, \ldots, K^{(e_1)}$ von $\mathfrak{M}_1$ bestehen. Der e_2-Schritt soll darin bestehen, daß man erzeugende Elemente $A^{(1)}, A^{(2)}, \ldots$ von $\mathfrak{A}_1$ bestimmt und die so bekanntgewordene Matrix $\mathfrak{M}_1$ in (14) nach den Zeilen reduziert. Der e_n-Schritt ($n = 3, \ldots, \nu+1$) soll darin bestehen, daß man von einer nach den Zeilen reduzierten Matrix M_{n-2} ausgehend, diese ausreduziert, dann die zu den Diagonalelementen -1 gehörenden Zeilen und Spalten streicht, und in der übriggebliebenen Matrix den Index $n-2$ der Elemente zu $n-1$ erhöht, endlich die so gewonnene Matrix M_{n-1} (die eine Ableitung von M_{n-2} ist) nach den Zeilen reduziert. Man sieht, daß die so definierten e_1-, $\ldots$, $e_{\nu+1}$-Schritte offenbar den ganzen Algorithmus ausmachen und im allgemeinen durch den e_n-Schritt die Zahl $e_n (= e_{n-1} - r_n)$ bekannt wird.[25]

§ 4. Lemmas und weitere Sätze

Wir sprechen hier noch die folgenden Lemmas und Sätze aus, die wir mit den Sätzen 1, 2, dem Hauptsatz und Zusatz vom § 2 zusammen erst im § 5 beweisen.

LEMMA 1. *Es gelten die Formeln*

$$(17) \qquad O(\mathfrak{A}_n) = l^{e_n}, \quad O(\mathfrak{M}_n) = \frac{l^{e_n} - 1}{l - 1}, \quad g(\Pi_n | \Omega) = l^{e_n}.$$

Die Menge $\mathfrak{M}_n$ ist in dem Sinne abgeschlossen, daß alle $K (\subset \Pi_n)$ wieder zu $\mathfrak{M}_n$ gehören. Eine Basis von $\mathfrak{A}_n$ und auch von $\mathfrak{M}_n$ besteht aus e_n Elementen.

[25] Man berücksichtige, daß insbesondere der $e_{\nu+1}$-Schritt zu einer nach den Zeilen reduzierten Matrix M_ν führt, in der alle Diagonalelemente gleich -1 sind, die also offenbar auch schon ausreduziert ist. Somit bedeutet der $e_{\nu+1}$-Schritt in der Tat, daß der Algorithmus mit ihm schon beendet ist.

Lemma 2. *Gehöre zu einem* K *im Sinne der Klassenkörpertheorie die Untergruppe* $\mathfrak{h}$ *vom Index* l *von* $\mathfrak{H}$.[26] *Dann und nur dann gilt* $\mathsf{K} \in \mathfrak{M}_n$, *wenn*[27]

$$\mathfrak{h}^{l^{n-1}} \neq \mathfrak{H}^{l^{n-1}} \tag{18}$$

ist. (Vgl. Satz 4.)

Lemma 3. *Das bedingte Artinsche Symbol* $\left(\frac{\mathsf{K}}{C}\right)_n$ *existiert dann und nur dann, wenn*

$$\mathsf{K} \in \mathfrak{M}_n, \; C \in \mathfrak{H}^{l^{n-1}} \tag{19}$$

gelten. In diesem Falle ist dann und nur dann

$$\left(\frac{\mathsf{K}}{C}\right)_n = 1, \tag{20}$$

wenn

$$C \in \mathfrak{h}^{l^{n-1}} \tag{21}$$

gilt, wobei $\mathfrak{h}$ *dasselbe bedeutet, wie im Lemma 2.* (Vgl. Satz 5.) *Insbesondere existiert also* $\left(\frac{\mathsf{K}}{A}\right)_n$ *dann und nur dann, wenn*

$$\mathsf{K} \in \mathfrak{M}_n \quad A \in \mathfrak{A}_n \tag{22}$$

gelten.

Satz 3. *Über einem* K_n *existiert dann und nur dann mindestens ein* K_{n+1}, *wenn*[28]

$$\left(\frac{\mathsf{K}_n}{A}\right) = 1 \tag{23}$$

für alle A *gilt.*[29]

Satz 4. *Zu einem Paar* $(n \geqq 2)$, K *gibt es ein* K_n *über* K *(d. h.* K *gehört in* $\mathfrak{M}_n$*) dann und nur dann, wenn es über* K *mindestens ein* K_{n-1} *gibt (d. h.* K *in* $\mathfrak{M}_{n-1}$ *gehört) und*

$$\left(\frac{\mathsf{K}}{A}\right)_{n-1} = 1 \tag{24}$$

für diejenigen A *gilt, für die die linke Seite existiert.* (Ein Gegenstück zu Satz 3.)

[26] Obige Redeweise ist nicht ganz korrekt, gibt aber zu keinem Mißverständnis Anlaß. Genau gesprochen meinen wir mit $\mathfrak{h}$ die Gruppe derjenigen Klassen, die sich aus den Elementen der zu K gehörenden Idealgruppe bilden lassen.

[27] Für eine Abelsche Gruppe G bezeichnet G^r die Gruppe der r-ten Potenzen der Elemente von G.

[28] Die rechte Seite 1 von (23) bezeichnet den identischen Automorphismus von K_n.

[29] Obiger Satz nebst Formel (17) rührt für den Spezialfall der absoluten Klassengruppe eines quadratischen Zahlkörpers von Reichardt [8] her. Dieser Satz kommt bei uns erst im § 6 zur Anwendung.

Satz 5. *Das bedingte Artinsche Symbol* $\left(\frac{\mathsf{K}}{C}\right)_n$ $(n \geqq 2)$ *existiert dann und nur dann, wenn es über* K *mindestens ein* K_n *gibt (d. h.* $\mathsf{K} \in \mathfrak{M}_n$ *gilt) und* $\left(\frac{\mathsf{K}}{C}\right)_{n-1}$ *existiert, ferner die Bedingung*

$$\left(\frac{\mathsf{K}'}{C}\right)_{n-1} = 1 \tag{25}$$

für diejenigen K' *erfüllt ist, für die die linke Seite existiert.*

§ 5. Beweis

Hier beweisen wir unsere Lemmas (in § 4), Sätze (in §§ 2, 4), den Hauptsatz und Zusatz (in § 2). Wir machen einige Vorbereitungen.

Stets bezeichne $\mathfrak{h}_n$ eine Untergruppe von $\mathfrak{H}$, wofür $\mathfrak{H}/\mathfrak{h}_n$ zyklisch von der Ordnung l^n ist. Insbesondere für $\mathfrak{h}_1$ schreiben wir auch $\mathfrak{h}$, wie schon in den Lemmas 2, 3. Bekanntlich sind die K_n und $\mathfrak{h}_n$ im Sinne der Klassenkörpertheorie einander paarweise zugeordnet.

Mit (χ) bezeichnen wir die Gruppe aller Charaktere von $\mathfrak{H}$. Selbst χ soll ein beliebiges Element von (χ) bezeichnen. Mit (χ^r) werde die Untergruppe von (χ) bezeichnet, die aus den χ^r besteht, wofür also $(\chi^r) = (\chi)^r$ gilt.

Mit λ_n bezeichnen wir ein beliebiges Element l^n-ter Ordnung von (χ). Insbesondere für λ_1 schreiben wir auch λ. Bekanntlich (vgl. Hasse [2]) sind die Untergruppen G von $\mathfrak{H}$ und die Untergruppen G' von (χ) einander paarweise zugeordnet, wenn dabei G die Gruppe derjenigen C bedeutet, für die $\chi(C) = 1$ $(\chi \in G')$ gilt. Es gilt auch die Isomorphie $\mathfrak{H}/G \approx G'$. Hiernach sind insbesondere die $\mathfrak{h}_n$ und $\{\lambda_n\}$ einander zugeordnet. Noch spezieller (Fall $n = 1$) sind auch die $\mathfrak{h}$ und $\{\lambda\}$ einander zugeordnet. Ferner gehören offenbar $\mathfrak{A}_1$ und (χ^l) einander zu.

Wir betrachten einem Klassenkörper stets auch diejenige Untergruppe von (χ) als zugeordnet, die der ihm zugeordneten Untergruppe von $\mathfrak{H}$ entspricht. Diese Zuordnung ist monoton, d. h. für zwei Klassenkörper A_1, A_2 und die zugeordnete Untergruppen G_1, G_2 von (χ) bedingen $A_1 \subset A_2$ und $G_1 \subset G_2$ einander gegenseitig. Insbesondere sind die K_n und $\{\lambda_n\}$ einander zugeordnet.

Beweis von Lemma 1. Die Formel (17_1) folgt sofort aus der Definition von $\mathfrak{A}_n$ und der Theorie der endlichen Abelschen Gruppen.

Nach obigem sind die Körper $\mathsf{K}(\in \mathfrak{M}_n)$ und die Gruppen $\{\lambda_n^{l^{n-1}}\}$ einander zugeordnet. Diese Gruppen stimmen mit den Untergruppen l-ter Ordnung der Gruppe $(\chi^{l^{n-1}}) = (\chi)^{l^{n-1}}$ überein. Da diese Gruppe isomorph mit $\mathfrak{H}^{l^{n-1}}$ ist und letztere Gruppe genau e_n Invarianten hat, so ist die Anzahl der genannten Untergruppen bekanntlich gleich der rechten Seite von (17_2), womit diese Formel bewiesen ist.

Ferner folgt aus dem Gesagten, daß der Körper Π_n und die durch alle $\lambda_n^{l^{n-1}}$ erzeugte Gruppe einander zugeordnet sind. Letztere Gruppe besteht aus denjenigen Elementen von $(\chi)^{l^{n-1}}$, die von der Ordnung $\leqq l$ sind. Die Anzahl dieser Elemente ist l^{e_n}, woraus (17_3) folgt.

Die Abgeschlossenheit der Körpermenge $\mathfrak{M}_n$ ergibt sich daraus, daß umgekehrt alle Untergruppen l-ter Ordnung von $(\chi)^{l^{n-1}}$ von der Form $\{\lambda_n^{l^{n-1}}\}$ sind.

Aus (17_1), (17_3) folgen auch die Behauptungen über die Basen von $\mathfrak{A}_n$ und Π_n, womit Lemma 1 bewiesen ist.

Beweis von Lemma 2. Zuerst nehmen wir $K \in \mathfrak{M}_n$ an. Das bedeutet, daß $\mathfrak{h}$ eine Untergruppe $\mathfrak{h}_n$ enthält. Für diese gilt in einer selbstverständlichen Schreibweise die Zerlegung in Nebengruppen

(26) $$\mathfrak{H} = (H, X, X^2, \ldots, X^{l^n-1})\mathfrak{h}_n$$

mit einem geeigneten $X(\in \mathfrak{H})$. Wegen $\mathfrak{h}_n \subseteqq \mathfrak{h}$ und $O(\mathfrak{H}/\mathfrak{h}) = l$ folgt hieraus

(27) $$\mathfrak{h} = (H, X^l, X^{2l}, \ldots, X^{l^n-l})\mathfrak{h}_n.$$

Wegen (26) ist $X^{l^n} \in \mathfrak{h}_n$, weshalb sich nach (27)

(28) $$\mathfrak{h}^{l^{n-1}} \subseteqq \mathfrak{h}_n$$

ergibt. Wegen (26) gehört $X^{l^{n-1}}$ nicht in $\mathfrak{h}_n$, also nach (28) noch weniger in $\mathfrak{h}^{l^{n-1}}$, woraus (18) folgt.

Nehmen wir umgekehrt (18) an. Es gehöre $\mathfrak{h}$ die Untergruppe $\{\lambda\}$ von (χ) zu. Andererseits gehören $\mathfrak{h}^{l^{n-1}}$ und $\mathfrak{H}^{l^{n-1}}$ offenbar die Gruppen G' und G'' derjenigen Charaktere χ zu, für die $\chi^{l^{n-1}}$ in $\{\lambda\}$ liegt, bzw. dem Hauptcharakter 1 gleich ist. Wegen (18) gilt $G' \neq G''$, somit gibt es ein χ mit

$$\chi^{l^{n-1}} \in \{\lambda\}, \neq 1.$$

Dann ist χ von der Ordnung l^n, ferner gilt $\{\chi\} \supseteqq \{\lambda\}$, weshalb zu $\{\chi\}$ ein $\mathfrak{h}_n$ $(\subseteqq \mathfrak{h})$ gehört. Dies bedeutet $K \in \mathfrak{M}_n$, womit Lemma 2 bewiesen ist.

Zu späteren Zwecken bemerken wir, daß die linke Seite von (18) für die verschiedenen $K(\in \mathfrak{M}_n)$ verschieden ist. Wir haben nämlich gesehen, daß zu $\mathfrak{h}^{l^{n-1}}$ die Gruppe derjenigen Charaktere χ zugeordnet ist, für die $\chi^{l^{n-1}} \in \{\lambda\}$ ist, woraus die Richtigkeit der Behauptung folgt.

Beweis von Lemma 3. Als Vorbereitung beweisen wir, daß wenn $\mathfrak{h}$ für ein festes n mindestens ein $\mathfrak{h}_n$ enthält, dann die $\mathfrak{h}_n$ $(\subseteqq \mathfrak{h})$ eben $\mathfrak{h}^{l^{n-1}}$ zum Durchschnitt haben.

Es gehöre nämlich $\mathfrak{h}$ zu $\{\lambda\}$. Der genannte Durchschnitt gehört dann zu der durch diejenigen λ_n erzeugten Gruppe, für die $\lambda_n^{l^{n-1}} = \lambda$ gilt. Diese Gruppe wird auch durch die χ mit $\chi^{l^{n-1}} \in \{\lambda\}$ erzeugt, ist also gerade die Gruppe G' im vorigen Beweis von Lemma 2. Da G' zu $\mathfrak{h}^{l^{n-1}}$ gehört, so ist die Behauptung richtig.

Zur Existenz von $\left(\frac{K}{C}\right)_n$ ist wegen der Definition vor allem nötig, daß (19_1) gilt. Deshalb dürfen wir beim Beweis von Lemma 3 das Erfülltsein von (19_1) von vornherein annehmen. Hieraus folgt nach Lemma 2 auch die Gültigkeit von (18).

Wir schicken noch die Bemerkung voran, daß die $K_n(\supseteqq K)$ und $\mathfrak{h}_n(\subseteqq \mathfrak{h})$ offenbar einander zugeordnet sind.

Nunmehr wollen wir zuerst zeigen, daß (unter der gemachten Annahme (19_1)) die Aussagen (20), (21) äquivalent sind. Wegen der Definition des bedingten Artinschen Symbols und einer Grundeigenschaft des Artinschen Symbols bedeutet (20) nach der eben gemachten Bemerkung, daß C in allen $\mathfrak{h}_n(\subseteqq \mathfrak{h})$, d. h. in ihrem Durchschnitt $\mathfrak{h}^{l^{n-1}}$ liegt. Damit haben wir die behauptete Äquivalenz von (20), (21) bewiesen. Da (19_2) eine Folgerung von (21) ist, so steht das gewonnene Resultat mit Lemma 3 im Einklang.

Im übrigen Teil des Beweises dürfen wir also (neben der schon früher gemachten Annahme (19_1)) auch noch annehmen, daß (21) nicht gilt, und dann haben wir nur noch zu beweisen, daß (19_2) notwendig und hinreichend zur Existenz von $\left(\frac{K}{C}\right)_n$ ist.

Erstens nehmen wir (19_2) an. Dann ist C eine l^{n-1}-te Potenz, somit sind alle $\left(\frac{K_n}{C}\right)$ mit $K_n \supseteqq K$ von einer Ordnung $\leqq l$. Wir haben also wegen der Definition des bedingten Artinschen Symbols nur zu zeigen, daß die gesagten $\left(\frac{K_n}{C}\right)$ ungleich 1 sind, d. h. C außerhalb aller $\mathfrak{h}_n(\subseteqq \mathfrak{h})$ liegt.

Zu diesem Zweck setzen wir wieder (26) an, woraus auch (27) folgt. Dies ergibt

$$\mathfrak{H} = (H, X, X^2, \ldots, X^{l-1})\,\mathfrak{h}.$$

Da wegen (19_1) auch (18) gilt, so folgt hieraus

$$\mathfrak{H}^{l^{n-1}} = (H, X^{l^{n-1}}, X^{2l^{n-1}}, \ldots, X^{(l-1)l^{n-1}})\,\mathfrak{h}^{l^{n-1}}.$$

Da ferner (21) nicht gilt, so ergibt sich

$$C \in X^{il^{n-1}}\,\mathfrak{h}^{l^{n-1}}$$

mit einem i $(=1, \ldots, l-1)$. Auf der rechten Seite liegt der erste Faktor nach (26) in keinem $\mathfrak{h}_n(\subseteqq \mathfrak{h})$, während der zweite Faktor nach obigem in allen $\mathfrak{h}_n(\subseteqq \mathfrak{h})$ enthalten ist. Hiernach liegt C außerhalb aller $\mathfrak{h}_n(\subseteqq \mathfrak{h})$, was wir zu zeigen hatten.

Zweitens nehmen wir die Existenz von $\left(\frac{K}{C}\right)_n$ an. Da (21) nicht gilt, so ist dieses Symbol gleich -1. Das bedeutet, daß $\left(\frac{K_n}{C}\right)$ für alle $K_n(\supseteqq K)$ von

l-ter Ordnung ist. Folglich gilt

(29) $$C \notin \mathfrak{h}_n$$

und $C^l \in \mathfrak{h}_n$ für alle $\mathfrak{h}_n (\subseteq \mathfrak{h})$. Aus letzterem folgt nach obigem

(30) $$C^l \in \mathfrak{h}^{l^{n-1}}$$

Nehmen wir noch an, daß (19_2) falsch, d. h.

(31) $$C \notin \mathfrak{H}^{l^{n-1}}$$

ist. Wir werden aus (29) bis (31) einen Widerspruch ableiten, womit der Beweis beendet wird.

Gehöre $\mathfrak{h}$ zu $\{\lambda\}$. Dann bedeuten (29) bis (31) der Reihe nach:

1) $\lambda_n(C) \neq 1$ für jedes λ_n mit $\lambda_n^{l^{n-1}} = \lambda$.

2) $\chi(C^l) = 1$ für jedes χ mit $\chi^{l^{n-1}} \in \{\lambda\}$.

3) $\lambda_{n-1}(C) \neq 1$ für mindestens ein λ_{n-1}.

Wegen 1), 2) ist $\lambda_n(C)$ eine Einheitswurzel l-ter Ordnung, also gibt es nach 3) ein λ_{n-1} und ein i derart, daß

$$\lambda_n(C)\lambda_{n-1}^i(C) = 1.$$

Dies bedeutet $\lambda_n'(C) = 1$ für $\lambda_n' = \lambda_n \lambda_{n-1}^i$. Da aber $\lambda_n'^{l^{n-1}} = \lambda_n^{l^{n-1}} = \lambda$ gilt, so sind wir zu einem Widerspruch mit 1) gekommen. Das beweist Lemma 3.

Beweis von Satz 1. Bezeichne G eine beliebige Untergruppe von $\mathfrak{H}$. Liegen zwei der im Satz 1 genannten $l+1$ Klassen C'' in G, so tun das alle. Wenden wir dies mit $G = \mathfrak{H}^{l^{n-1}}$ an, so folgt aus der ersten Aussage im Lemma 3 sofort die Richtigkeit der ersten Behauptung von Satz 1. Die Anwendung des vorigen mit $G = \mathfrak{h}^{l^{n-1}}$ und die zweite Aussage im Lemma 3 lehren, daß alle Symbole (9) gleich 1 sind, wenn das für irgend zwei dieser Symbole gilt.

Zum vollständigen Beweis von Satz 1 brauchen wir nur noch zu zeigen, daß mindestens eins der Symbole (9) gleich 1 ist, wenn alle existieren. Nun bedeutet diese Annahme wieder nach der ersten Aussage im Lemma 3, daß

(32) $$K \in \mathfrak{M}_n$$

und für alle C'' in (9)

(33) $$C'' \in \mathfrak{H}^{l^{n-1}}$$

gilt. Da die K zugeordnete Untergruppe $\mathfrak{h}$ vom Index l ist, so hat $\mathfrak{h}^{l^{n-1}}$ den Index 1 oder l in der rechten Seite von (33), somit folgt aus (33) offenbar, daß für mindestens eins der genannten C'' sogar

$$C'' \in \mathfrak{h}^{l^{n-1}}$$

gilt. Dies und (32) besagen nach der zweiten Aussage im Lemma 3 eben die Richtigkeit des übriggebliebenen Teils von Satz 1, womit dieser Satz vollständig bewiesen ist.

Beweis von Satz 2. Aus der im Lemma 1 bewiesenen Abgeschlossenheit von $\mathfrak{M}_n$ folgt für die im Satz 2 genannten $l+1$ Körper K'', daß sie alle in $\mathfrak{M}_n$ liegen, wenn das für zwei unter ihnen gilt. Hieraus folgt nach der ersten Aussage im Lemma 3 die Richtigkeit der ersten Behauptung von Satz 2.

Wir bezeichnen mit $\mathfrak{h}, \mathfrak{h}'$ die K bzw. K' zugeordnete Untergruppe von $\mathfrak{H}$. Diese sind vom Index l und voneinander verschieden, also ist ihr Durchschnitt

(34) $$\mathfrak{d} = \mathfrak{h} \cap \mathfrak{h}'$$

vom Index l^2 in $\mathfrak{H}$ mit nichtzyklischer Faktorgruppe $\mathfrak{H}/\mathfrak{d}$. Bezeichnet noch $\mathfrak{h}''$ die K'' zugeordnete Untergruppe von $\mathfrak{H}$, so durchläuft $\mathfrak{h}''$ eben die $l+1$ Untergruppen von $\mathfrak{H}$ mit der Eigenschaft

$$\mathfrak{d} \subset \mathfrak{h}'' \subset \mathfrak{H}.$$

Hieraus folgt

(35) $$\mathfrak{d}^{l^{n-1}} \subseteqq \mathfrak{h}''^{l^{n-1}} \subseteqq \mathfrak{H}^{l^{n-1}}.$$

Nehmen wir nunmehr an, daß die Symbole (10) existieren. Nach Lemma 2 und der ersten Aussage im Lemma 3 ist dann das zweite „=" Zeichen in (35) unmöglich. Nach der dem Beweis von Lemma 2 angefügten Bemerkung sind die Gruppen in der Mitte von (35) für die verschiedenen $\mathfrak{h}''$ verschieden. Diese haben den Index l in der rechten Seite von (35), somit hat die linke Seite von (35) einen Index $\geqq l^2$ in der rechten Seite. Wegen (34) muß dieser Index genau l^2 sein, zugleich schreibt sich (35) genauer als

(36) $$\mathfrak{d}^{l^{n-1}} \subset \mathfrak{h}''^{l^{n-1}} \subset \mathfrak{H}^{l^{n-1}}.$$

Es ist auch klar, daß die $l+1$ verschiedenen Gruppen in der Mitte von (36) paarweise die linke Seite zum Durchschnitt haben und ihre Vereinigungsmenge gleich der rechten Seite ist. Wenn also C irgendeine Klasse in der rechten Seite von (36) ist, so ist diese entweder in allen Gruppen $\mathfrak{h}''^{l^{n-1}}$ oder in genau einer dieser Gruppen enthalten. Dies bedeutet nach der zweiten Aussage in Lemma 3 eben die Richtigkeit des übriggebliebenen Teils von Satz 2, womit wir diesen Satz bewiesen haben.

Beweis von Satz 3. Die Behauptung dieses Satzes läßt sich offenbar so aussprechen: Ein $\mathfrak{h}_n$ enthält dann und nur dann mindestens ein $\mathfrak{h}_{n+1}$, wenn $\mathfrak{A}_1 \subseteqq \mathfrak{h}_n$ gilt.

Erstens nehmen wir ein Gruppenpaar $\mathfrak{h}_n, \mathfrak{h}_{n+1}$ mit $\mathfrak{h}_n \supset \mathfrak{h}_{n+1}$ an. Wir zerlegen $\mathfrak{H}$ in Nebengruppen

(37) $$\mathfrak{H} = (H, X, X^2, \ldots, X^{l^{n+1}-1})\, \mathfrak{h}_{n+1}$$

mit Hilfe einer passenden Klasse X. Dann muß gelten:

(38) $$\mathfrak{h}_n = (H, X^{l^n}, X^{2l^n}, \ldots, X^{(l-1)l^n})\, \mathfrak{h}_{n+1}.$$

Wegen (37) schreibt sich jedes A in der Form

(39) $$A = X^i Y. \qquad (Y \in \mathfrak{h}_{n+1})$$

Aus $A^l = H$, $Y^l \in \mathfrak{h}_{n+1}$ folgt $X^{il} \in \mathfrak{h}_{n+1}$. Nach (37) gilt also $l^{n+1} | il$, $l^n | i$. Wegen (38), (39) folgt hieraus $A \in \mathfrak{h}_n$, also gilt $\mathfrak{A}_1 \subseteq \mathfrak{h}_n$.

Zweitens nehmen wir umgekehrt $\mathfrak{A}_1 \subseteq \mathfrak{h}_n$ für ein $\mathfrak{h}_n$ an. Dies bedeutet $(\chi^l) \subseteq \{\lambda_n\}$, wobei die rechte Seite die $\mathfrak{h}_n$ zugeordnete Untergruppe von (χ) ist. Hieraus folgt

$$\lambda_n = \chi^l \tag{40}$$

mit einem passenden χ, ferner muß dann χ von der Ordnung l^{n+1}, d. h. gleich einem λ_{n+1} sein. Hierfür gilt wegen (40) auch $\{\lambda_{n+1}\} \supset \{\lambda_n\}$, somit ist die der linken Seite zugeordnete Untergruppe $\mathfrak{h}_{n+1}$ in $\mathfrak{h}_n$ enthalten. Satz 3 haben wir bewiesen.

Beweis von Satz 4. Wir dürfen $K \in \mathfrak{M}_{n-1}$ annehmen, da sonst $K \in \mathfrak{M}_n$ unmöglich ist, und dann haben wir zu beweisen, daß die bei (24) ausgesprochene Bedingung notwendig und hinreichend ist, damit $K \in \mathfrak{M}_n$ gilt.

Wieder gehöre K zur Untergruppe $\mathfrak{h}$ von $\mathfrak{H}$. Nach Lemma 3 ist (in einer von selbst klaren Schreibweise)

$$A \in \mathfrak{H}^{l^{n-2}} - \mathfrak{h}^{l^{n-2}} \tag{41}$$

notwendig und hinreichend, damit $\left(\frac{K}{A}\right)_{n-1} = -1$ ist. (Dabei ist die rechte Seite von (41) wegen $K \in \mathfrak{M}_{n-1}$ und Lemma 2 nicht leer.) Nach Lemma 2 genügt es also zu zeigen, daß (41) dann und nur dann für kein A gilt, wenn

$$\mathfrak{h}^{l^{n-1}} \neq \mathfrak{H}^{l^{n-1}} \tag{42}$$

ist.

Erstens nehmen wir an, daß (41) für kein A gilt. Das bedeutet, daß die rechte Seite von (41) aus lauter Elementen von einer Ordnung $\geqq l^2$ besteht. Dann läßt sich

$$\mathfrak{H}^{l^{n-2}} = (H, X, X^2, \ldots, X^{l-1})\, \mathfrak{h}^{l^{n-2}} \tag{43}$$

setzen, so daß X ein Element aus einer Basis der linken Seite ist und eine Ordnung $\geqq l^2$ hat. Da ferner X nicht in $\mathfrak{h}^{l^{n-2}}$ gehört, so folgt leicht, daß X^l nicht in $\mathfrak{h}^{l^{n-1}}$ gehören kann, also (42) gilt.

Zweitens nehmen wir das Gegenteil an, daß nämlich (41) für ein A gilt. Hieraus folgt

$$\mathfrak{H}^{l^{n-2}} = (H, A, A^2, \ldots, A^{l-1})\, \mathfrak{h}^{l^{n-2}},$$

und weiter hieraus folgt wegen $A^l = H$ auch $\mathfrak{H}^{l^{n-1}} = \mathfrak{h}^{l^{n-1}}$, d. h. das Nichtbestehen von (42). Wir haben Satz 4 bewiesen.

Beweis von Satz 5. Wir dürfen gleich $K \in \mathfrak{M}_n$ annehmen, da sonst $\left(\frac{K}{C}\right)_n$ nach Lemma 3 nicht existiert.

Erstens nehmen wir die Existenz von $\left(\frac{K}{C}\right)_n$ an. Nach Lemma 3 gilt dann

$$C = X^{l^{n-1}}$$

mit einer Klasse X. Existiert also irgendein $\left(\frac{K'}{C}\right)_{n-1}$ — was insbesondere für $K' = K$ gewiß der Fall ist — und gehört K' zu einer Untergruppe $\mathfrak{h}'$ von $\mathfrak{H}$, so gilt wegen $O(\mathfrak{H}/\mathfrak{h}') = l$ auch $X^l \in \mathfrak{h}'$, also $C \in \mathfrak{h}'^{l^{n-2}}$. Hieraus folgt nach Lemma 3 das Bestehen von $\left(\frac{K'}{C}\right)_{n-1} = 1$.

Zweitens nehmen wir an, daß $\left(\frac{K}{C}\right)_n$ nicht existiert. Dann gibt es nach Lemma 3 eine größte ganze Zahl r mit

$$C \in \mathfrak{H}^{l^r} \qquad (0 \leqq r \leqq n-2).$$

Im Fall $r < n-2$ sind wir mit dem Beweis fertig, da dann $\left(\frac{K}{C}\right)_{n-1}$ nach demselben Lemma nicht existiert. Es bleibt also nur noch der Fall

$$C = X^{l^{n-2}} \tag{44}$$

zu betrachten, wobei X eine Klasse bezeichnet, die keine l-te Potenz ist. Die Ordnung von X ist mindestens l^{n-1}, da sonst $C = H$ wäre, was ja unmöglich ist. Es gibt also einen Charakter λ_{n-1}, so daß $\lambda_{n-1}(X)$ eine Einheitswurzel l^{n-1}-ter Ordnung ist. Zu $\{\lambda_{n-1}\}$ gehört eine Untergruppe $\mathfrak{h}_{n-1}$ von $\mathfrak{H}$, die dann in einer Gruppe $\mathfrak{h}$ enthalten ist. Diese gehört zu $\{\lambda_{n-1}^{l^{n-2}}\}$. Es seien K', K'_{n-1} die bzw. zu $\mathfrak{h}, \mathfrak{h}_{n-1}$ gehörenden Körper ($K' \subseteq K'_{n-1}$). Nach Lemma 2 (angewendet auf K' statt K) ist wegen $K' \in \mathfrak{M}_{n-1}$:

$$\mathfrak{h}^{l^{n-2}} \neq \mathfrak{H}^{l^{n-2}} \tag{45}$$

Wegen $\lambda_{n-1}^{l^{n-2}}(X) \neq 1$ liegt X nicht in $\mathfrak{h}$, somit folgt aus (44), (45) offenbar, daß C nicht in $\mathfrak{h}^{l^{n-2}}$ liegt. Dies und (44) besagen nach Lemma 3, daß $\left(\frac{K'}{C}\right)_{n-1} = -1$ ist. Satz 5 haben wir in allen Fällen bewiesen.

Beweis des Hauptsatzes. Nach Lemma 1 besteht eine Basis von $\mathfrak{A}_1$ und auch von $\mathfrak{M}_1$ aus je e_1 Elementen. Hiernach hat die Matrix M_1 in (14) mindestens e_1 Zeilen und genau e_1 Spalten. Gleich bemerken wir, daß also nach dem Bildungsgesetz der Ableitung alle Matrizen in (15) mindestens soviel Zeilen wie Spalten enthalten.

Wir setzen für ein festes n voraus, daß M_1 $n-1$-mal ableitbar ist und in jeder $n-1$-ten Ableitung M_n von M_1 die Nenner und Zähler erzeugende Elemente von $\mathfrak{A}_n$ bzw. eine Basis von $\mathfrak{M}_n$ bilden, woraus nach Lemma 1 schon folgt, daß M_n mindestens e_n Zeilen und genau e_n Spalten hat. Die Voraussetzung ist nach obigem insbesondere für $n = 1$ erfüllt. Wir zeigen, daß aus ihr die ähnliche Aussage für $n+1$ statt n folgt, womit wir den Hauptsatz bewiesen haben werden.

Betrachten wir eine beliebige der genannten Matrizen M_n und nehmen diese so an:

$$
(46) \qquad M_n = \left|\begin{matrix} \left(\dfrac{K^{(1)}}{A^{(1)}}\right)_n & \cdots & \left(\dfrac{K^{(e_n)}}{A^{(1)}}\right)_n \\ \left(\dfrac{K^{(1)}}{A^{(2)}}\right)_n & \cdots & \left(\dfrac{K^{(e_n)}}{A^{(2)}}\right)_n \\ \vdots & & \end{matrix}\right|
$$

(Diese $A^{(i)}$ und $K^{(i)}$ sind im Fall $n > 1$ nicht dieselben wie im Hauptsatz, aber es wird kein Mißverständnis entstehen, da wir es im Beweis nur noch mit (46) zu tun haben werden.) Es genügt zu zeigen, daß jede (formale) Ableitung M_{n+1} wirklich existiert und in ihr die Nenner und Zähler erzeugende Elemente von $\mathfrak{A}_{n+1}$ bzw. eine Basis von $\mathfrak{M}_{n+1}$ bilden. Im Falle $n > \nu$ ist M_n leer, also auch M_{n+1} leer, weshalb die Behauptung für diesen Fall richtig ist. Wir brauchen nur noch den Fall $n \leqq \nu$ zu betrachten. Zur Bildung einer Matrix M_{n+1} haben wir M_n zuerst auszureduzieren. Wir wollen die Bezeichnung (46) nach dem Ausreduzieren behalten. Bezeichne dann s die Anzahl der Elemente 1 in der Diagonale von M_n. Diese sind die ersten s Elemente der Diagonale. Außer den übrigen $e_n - s$ Diagonalelementen -1 hat M_n lauter Elemente 1.

Hiernach folgt aus den Sätzen 1, 2 sofort, daß

$$
(47) \qquad \left(\frac{K}{A}\right)_n
$$

bei festem $K(\in \mathfrak{M}_n)$ für alle $A(\in \mathfrak{A}_n)$ bzw. bei festem $A(\in \mathfrak{A}_n)$ für alle $K(\in \mathfrak{M}_n)$ dann und nur dann 1 ist, wenn

$$
(48) \qquad K \subseteq K^{(1)} \dots K^{(s)},
$$

bzw.

$$
(49) \qquad A \in \{A^{(1)}, \dots, A^{(s)}, A^{(e_n+1)}, \dots\}
$$

gilt.

Berücksichtigen wir auch, daß (47) nach dem Schluß von Lemma 3 eben nur für die $K(\in \mathfrak{M}_n)$, $A(\in \mathfrak{A}_n)$ definiert ist, so folgt aus der ersten obiger zwei Aussagen über (47) und aus dem (für $n+1$ statt n angewandten) Satz 4, daß die K in (48) eben $\mathfrak{M}_{n+1}$ ausmachen. Wegen der Unabhängigkeit von

$$
(50) \qquad K^{(1)}, \dots, K^{(s)}
$$

bilden also diese Körper eine Basis von $\mathfrak{M}_{n+1}$. Hieraus folgt nach Lemma 1 auch $s = e_{n+1}$. Insbesondere für $n = \nu$ bedeutet dies wegen $e_{\nu+1} = 0$, daß $M_{\nu+1}$ die leere Matrix ist. Da auch $\mathfrak{A}_{\nu+1}$, $\mathfrak{M}_{\nu+1}$ leer sind, so ist die Behauptung für diesen Fall richtig.

Ferner folgt im Fall $1 \leqq n \leqq \nu - 1$ aus der zweiten obiger zwei Aussagen und dem (für $n+1$ statt n angewandten) Satz 5, daß alle

$$
(51) \qquad \left(\frac{K}{A}\right)_{n+1} \quad (K \in \mathfrak{M}_{n+1};\ A \in \{A^{(1)}, \dots, A^{(s)}, A^{(e_n+1)}, \dots\})
$$

existieren.

Da nun eine beliebige der genannten Matrizen M_{n+1} so entsteht, daß man aus einer ausreduzierten Matrix M_n die zu den Diagonalelementen -1 gehörenden Zeilen und Spalten streicht, so lehren die gewonnenen Resultate, daß die Zähler (50) in M_{n+1} eine Basis von $\mathfrak{M}_{n+1}$ bilden und alle Elemente von M_{n+1} existieren (weil nämlich diese Elemente lauter Symbole (51) sind), d. h: selbst M_{n+1} existiert. Die Nenner in M_{n+1} sind aus den Nennern $A^{(1)}$, $A^{(2)}, \ldots$ in M_n so entstanden, daß man $(e_n - s =) e_n - e_{n+1}$ dieser Klassen gestrichen hat. Da ferner die Nenner in M_n die Gruppe $\mathfrak{A}_n$ erzeugen, so erzeugen die Nenner in M_{n+1} eine Gruppe, deren Ordnung mindestens

$$l^{-(e_n - e_{n+1})} O(\mathfrak{A}_n) = O(\mathfrak{A}_{n+1})$$

ist (vgl. (17_1)). Andererseits ist wegen (51) die gesagte Gruppe nach dem Schluß von Lemma 3 in $\mathfrak{A}_{n+1}$ enthalten, somit muß sie gleich $\mathfrak{A}_{n+1}$ sein. Alle Behauptungen über die (formalen) Ableitungen M_{n+1}, also auch den Hauptsatz haben wir bewiesen.

Beweis des Zusatzes. Man nehme M_ν als Fall $n = \nu$ von (46) gleich ausreduziert an. Bezeichne A den Nenner in einer der letzten $t - e_1$ Zeilen von M_ν. Wir haben $A = H$ zu beweisen. Da M_ν ausreduziert ist, so gilt

$$\left(\frac{K^{(i)}}{A}\right)_\nu = 1 \qquad (i = 1, \ldots, e_\nu).$$

Da diese $K^{(i)}$ nach dem Hauptsatz eine Basis von $\mathfrak{M}_\nu$ bilden, so folgt aus Satz 2 allgemeiner

$$\left(\frac{K}{A}\right)_\nu = 1 \qquad (K \in \mathfrak{M}_\nu).$$

Hieraus folgt nach den Lemmas 2, 3

$$A \in \mathfrak{h}^{l^{\nu-1}}$$

für alle Untergruppen $\mathfrak{h}$ vom Index l von $\mathfrak{H}$, für die

$$\mathfrak{h}^{l^{\nu-1}} \neq \mathfrak{H}^{l^{\nu-1}}$$

ist. Das bleibt auch nach der Aufhebung der letzteren Einschränkung trivial richtig. Es ist nun klar, daß der Durchschnitt aller $\mathfrak{h}^{l^{\nu-1}}$ gleich H ist, folglich gilt $A = H$. Damit ist der Zusatz bewiesen.

§ 6. Konstruktion

Hier wollen wir sehen, wie man auf Grund unseres Hauptsatzes den vollen Klassenkörper Ω_H konstruieren und hierdurch die Struktur der Klassengruppe $\mathfrak{H}$ effektiv bestimmen kann. Wir schicken zwei leichte Hilfssätze voran.

Hilfssatz 1. *Sind die zwei Artinschen Symbole*

$$\left(\frac{K_n}{C}\right), \quad \left(\frac{K_n}{C'}\right)$$

von der Ordnung l, so läßt sich ein i $(=1,\ldots,l-1)$ mit

$$\left(\frac{\mathsf{K}_n}{C}\right)^i\left(\frac{\mathsf{K}_n}{C'}\right)=1$$

bestimmen. Für dieses i gilt

$$\left(\frac{\mathsf{K}_n}{C''}\right)=1 \qquad (C''=C^iC')$$

HILFSSATZ 2. *Sind die zwei Artinschen Symbole*

$$\left(\frac{\mathsf{K}_n}{C}\right),\ \left(\frac{\mathsf{K}'_m}{C}\right) \qquad (n\geqq m\geqq 1)$$

von der Ordnung l, wobei keiner der Zähler im anderen enthalten ist, so läßt sich ein $\mathsf{K}''_n(\subset \mathsf{K}_n\mathsf{K}'_m)$ mit

$$\left(\frac{\mathsf{K}''_n}{C}\right)=1$$

folgenderweise bestimmen. Man nehme zwei Elemente ϱ,σ der Galoisschen Gruppe $\mathfrak{G}=\mathfrak{G}(\mathsf{K}_n\mathsf{K}'_m|\Omega)$ so, daß[30]

$$\varrho=\left(\frac{\mathsf{K}_n}{C}\right)\ \text{für}\ \mathsf{K}_n,\qquad \varrho=1\ \text{für}\ \mathsf{K}'_m,$$

$$\sigma=\left(\frac{\mathsf{K}'_m}{C}\right)\ \text{für}\ \mathsf{K}'_m,\qquad \sigma=1\ \text{für}\ \mathsf{K}_n$$

gelten, nehme dann eine Untergruppe $\mathfrak{G}_0$ von $\mathfrak{G}$, so daß $\mathfrak{G}_0$ das Element $\varrho\sigma$ enthält und die Faktorgruppe $\mathfrak{G}/\mathfrak{G}_0$ zyklisch von der Ordnung l^n ist. Dieser Untergruppe $\mathfrak{G}$ gehört im Sinne der Galoisschen Theorie ein passender Unterkörper K''_n von $\mathsf{K}_n\mathsf{K}'_m|\Omega$ zu. Man bemerke für den Fall $m<n$, daß dann $\mathsf{K}_n, \mathsf{K}''_n$ nicht unabhängig sind, d. h. einen gemeinsamen Körper K enthalten.

Hiervon bedarf Hilfssatz 1 keines Beweises.

Zum Beweis von Hilfssatz 2 sei vor allem bemerkt, daß die verlangten ϱ,σ gewiß existieren und von der Ordnung l sind. Die Existenz von $\mathfrak{G}_0$ ist auch klar. Ferner gilt für den $\mathfrak{G}_0$ zugeordneten Körper K''_n, daß $\mathsf{K}''_n|\Omega$ zyklisch vom Grade l^n ist. Wegen

$$\varrho\sigma=\left(\frac{\mathsf{K}_n}{C}\right)\left(\frac{\mathsf{K}'_m}{C}\right)=\left(\frac{\mathsf{K}_n\mathsf{K}'_m}{C}\right)$$

und $\mathsf{K}''_n\subset\mathsf{K}_n\mathsf{K}'_m$ ist $\varrho\sigma=\left(\frac{\mathsf{K}''_n}{C}\right)$ für K''_n. Wegen $\varrho\sigma\in\mathfrak{G}_0$ folgt hieraus $\left(\frac{\mathsf{K}''}{C}\right)=1$, womit Hilfssatz 2 bewiesen ist.

Die von uns gewünschte Konstruktion von Ω_H wird im wesentlichen in einer leichten Modifikation und Erweiterung des im § 3 beschriebenen Algorithmus bestehen, wobei wir uns Artinscher (statt bedingter Artinscher)

30 Oben soll man „für" als „bei Anwendung auf" deuten.

Symbole bedienen werden. Dabei werden die Hilfssätze 1, 2 statt der Sätze 1, 2 eintreten.

Wir betrachten für ein n $(=1, \ldots, \nu)$ zwei Systeme

$$A^{(1)}, \ldots, A^{(e_1+c)} \qquad (c \geqq 0), \tag{52}$$

$$\mathsf{K}_n^{(1)}, \ldots, \mathsf{K}_n^{(e_n)}, \mathsf{K}_{n-1}^{(e_n+1)}, \ldots, \mathsf{K}_{n-1}^{(e_{n-1})}, \ldots, \mathsf{K}_1^{(e_2+1)}, \ldots, \mathsf{K}_1^{(e_1)}, \tag{53}$$

wobei c eine feste (von n unabhängige) ganze Zahl ist, und bezeichnen die in den Körpern (53) enthaltenen K der Reihe nach mit

$$\mathsf{K}^{(1)}, \ldots, \mathsf{K}^{(e_1)}, \tag{54}$$

Zu unseren Zwecken beschränken wir uns auf den Fall, daß für jedes $k (=1, \ldots, n)$ die ersten e_k und die letzten c Klassen in (53) die Gruppe $\mathfrak{A}_k$ erzeugen, ferner die ersten e_k Körper in (54) eine Basis von $\mathfrak{M}_k$ bilden. Wir nennen dann (52), (53) zusammen kurz ein *n-stufiges System.*

Da die Körper (54) unabhängig sind, so sind es auch die Körper (53). Folglich hat das Produkt der letzteren den Grad $l^{e_1+\cdots+e_n}$ über Ω, somit ist dieses Produkt wegen

$$g(\Omega_n | \Omega) = l^{e_1+\cdots+e_n}. \tag{55}$$

eben der n-te Klassenkörper Ω_n. Wir werden unseren Algorithmus so einrichten, daß wir dabei nach und nach für jedes $n=1, \ldots, \nu$ ein n-stufiges System konstruieren, wodurch also nach und nach die Klassenkörper $\Omega_1, \ldots, \Omega_\nu$ bekannt werden. Da insbesondere $\Omega_\nu = \Omega_H$ ist, so wird das ein Verfahren zur Konstruktion des vollen Klassenkörpers. Dabei werden wir beim Aufstieg von einem $n-1$-stufigen System zu einem n-stufigen immer nur genau e_n elementare Körperkonstruktionen auszuführen brauchen $(n=2, \ldots, \nu)$, außerdem sind noch zur Aufstellung eines 1-stufigen Systems offenbar nur e_1 solche Konstruktionen nötig. Das sind insgesamt $e_1 + \cdots + e_\nu$ elementare Körperkonstruktionen. Der Vergleich mit dem Fall $n = \nu$ der Formel (55) zeigt, daß also unser Verfahren eine Mindestzahl von elementaren Körperkonstruktionen erfordern wird.

Um Klarheit zu schaffen, bemerken wir folgendes. Lassen wir C die ersten e_n und letzten c Klassen in (52), ferner A die ersten e_n Körper in (53) durchlaufen. Bilden wir aus diesen C und A die Matrix

$$M_n' = \left(\left(\frac{\mathsf{A}}{C} \right) \right) \tag{56}$$

vom Typ $(e_n + c) \times e_n$ mit den Elementen $\left(\frac{\mathsf{A}}{C} \right)$, wobei C und A den „Zeilen“ bzw. „Spaltenindex“ vertreten. Indem wir im allgemeinen einem Artinschen Symbol $\left(\frac{\mathsf{K}_n}{C} \right)$ das bedingte Artinsche Symbol $\left(\frac{\mathsf{K}}{C} \right)_n$ zuordnen, so entspricht der Matrix (56) durch diese Zuordnung eben eine Matrix M_n wie in unserem Hauptsatz, somit wird diese durch (56), also durch (52), (53) auch bekannt.

Kurz gesagt stehen die n-stufigen Systeme ($n = 1, 2, \ldots$) mit den im Hauptsatz genannten Matrizen $M_1, M_2, \ldots$ im Zusammenhang, daß durch jene auch diese bestimmt werden. Nun wird die gemeinte „Modifikation und Erweiterung“ unseres früheren Algorithmus so zustande kommen, daß wir Matrizen von der Art (56) betrachten, in denen wir aber C und Λ nunmehr *alle* Klassen und Körper in (52), (53) durchlaufen lassen und mit Hilfe dieser Matrizen nach und nach ein n-stufiges System ($n = 1, \ldots, \nu$) konstruieren werden.

Wie gesagt, betrachten wir die aus (52), (53) gebildete Matrix

$$M(n) = \left| \begin{matrix} \left(\dfrac{K_n^{(1)}}{A^{(1)}}\right) \cdots \left(\dfrac{K_1^{(e_1)}}{A^{(1)}}\right) \\ \left(\dfrac{K_n^{(1)}}{A^{(2)}}\right) \cdots \left(\dfrac{K_1^{(e_1)}}{A^{(2)}}\right) \\ \vdots \qquad\qquad \vdots \end{matrix} \right| = \left(\begin{array}{c|c} M_n' & \mathrm{I} \\ \hline \mathrm{II} & \mathrm{III} \end{array} \right) \tag{57}$$

vom Typ $(e_1 + c) \times e_1$ (die Nenner und Zähler der Elemente sind in unveränderter Reihenfolge die Klassen (52) bzw. die Körper (53)). Dann ist also die Matrix M_n' in (56) eine Teilmatrix von $M(n)$. Wir bezeichnen mit I, II, III die *erste, zweite* bzw. *dritte Komplementäre*[31] von M_n' in $M(n)$. Da M_n' nach obigem die Durchkreuzung der ersten e_n und letzten c Zeilen mit den ersten e_n Spalten von $M(n)$ ist, so ist auch die Bedeutung von I, II, III klar. Insbesondere ist III eine quadratische Matrix vom Typ $(e_1 - e_n) \times (e_1 - e_n)$.

Von jetzt an wollen wir nur solche n-stufigen Systeme in Betracht ziehen, für die alle Elemente von $M(n)$ von der Ordnung 1 oder l, insbesondere aber alle Elemente von I gleich 1 sind und III eine Diagonalmatrix mit lauter Elementen l-ter Ordnung in der Diagonale ist.[32]

Insbesondere erfüllt jedes 1-stufige System diese Forderungen, da im Fall $n = 1$ alle Elemente von $M(1)$ die Form $\left(\dfrac{K}{A}\right)$ haben und I, II, III leer sind. Wir nehmen deshalb an, daß wir für ein n $(=1, \ldots, \nu - 1)$ ein n-stufiges System (52), (53) von der verlangten Art schon aufgestellt haben, und wollen

[31] Eine Teilmatrix V einer Matrix U gibt Anlaß zu einer Aufspaltung von U in vier Teilmatrizen von der Form

$$U = \left(\begin{array}{c|c} V & \mathrm{I} \\ \hline \mathrm{II} & \mathrm{III} \end{array} \right).$$

Dann nennen wir I, II, III der Reihe nach die erste, zweite, dritte Komplementäre von V in U, und behalten diese Benennungen auch nach der Permutation der Zeilen und Spalten. (Genauer lassen sich die Teilmatrizen I, II, III so definieren: V und I oder II machen zusammen einige Zeilen bzw. Spalten von U aus, V, I, II, III machen zusammen U aus. Ist V leer, so ist III $= U$ und sind I, II leer, ist dagegen $V = U$, so sind I, II, III leer.)

[32] Diese Einschränkung steht uns frei, da es für unsere Zwecke genügt, für jedes n *ein* n-stufiges System aufzustellen.

mit Hilfe der zugehörigen Matrix $M(n)$ ein ähnliches System für $n+1$ (statt n) aufstellen, womit unsere Aufgabe (durch Induktion) erledigt sein wird.

Dieses Programm auszuführen ist ein leichtes. Vor allem verwandeln wir nämlich (53) in ein ähnliches System, wofür in der zugehörigen Matrix $M(n)$ auch die Teilmatrix II aus lauter Elementen 1 besteht und sonst der Wert der übrigen Elemente unverändert bleibt. Das kann wegen der obengesagten Eigenschaft der Teilmatrix III mit passender Anwendung von Hilfssatz 2 geschehen. Und zwar betrachten wir ein Element

$$\left(\frac{K_n}{A}\right) \neq 1 \tag{58}$$

von II und das in derselben Zeile stehende Diagonalelement

$$\left(\frac{K_m}{A}\right)$$

von III, das also ebenfalls $\neq 1$ ist. (Beide Symbole sind von der Ordnung l.) Ersetzt man dann in (53) und $M(n)$ den betrachteten Körper K_n nach Hilfssatz 2 durch einen Körper K_n'', so wird das Element (58) in $\left(\frac{K_n''}{A}\right) = 1$ verwandelt, während die Ordnung aller übrigen Elemente von $M(n)$ nach bekannter Eigenschaft der Artinschen Symbole offenbar unverändert bleibt. (Nebenbei bemerken wir, daß dadurch nach dem Schluß von Hilfssatz 2 in (54) keine Änderung eintritt.) Wird das für alle Fälle (58) nach und nach ausgeführt, so erreichen wir in der Tat, daß II lauter Elemente 1 hat, und I, III unverändert bleiben. Nach dieser „ersten Reduktion" behalten wir für $M(n)$ die alten Bezeichungen. Eine „zweite Reduktion" soll dann im wesentlichen im (vom § 2 her bekannten) Ausreduzieren von M_n bestehen, das aber jetzt an der Teilmatrix M_n' (statt M_n) auf Grund der Hilfssätze 1, 2 (statt der Sätze 1, 2) auszuführen wird. Wir meinen das so. Betrachten wir zwei Elemente

$$\left(\frac{K_n}{A}\right), \quad \left(\frac{K_n}{A'}\right) \tag{59}$$

$\neq 1$ in einer Spalte von M_n' oder zwei Elemente

$$\left(\frac{K_n}{A}\right), \quad \left(\frac{K_n'}{A}\right) \tag{60}$$

$\neq 1$ in einer Zeile von M_n'. Wird entsprechend A nach Hilfssatz 1 durch eine Klasse A'' bzw. K_n nach Hilfssatz 2 durch einen Körper K_n'' ersetzt, so läßt sich das erste Element von (59) bzw. (60) in 1 verwandeln. (Diese Ersetzungen denken wir natürlich jedesmal in (52), (53) also auch in $M(n)$ ausgeführt.) Die Elemente von I, II behalten dabei ihren Wert 1 offenbar, ferner wird an III überhaupt nichts geändert. Es ist klar, daß M_n' durch solche Ersetzungen und Permutationen gewisser Zeilen und Spalten von $M(n)$

in eine Diagonalmatrix übergeführt werden kann, in deren Diagonale die Elemente 1 den Elementen $\neq 1$ vorangehen. Wieder behalten wir auch nach dieser zweiten Reduktion die alten Bezeichungen bei. Wir sehen auch, daß nunmehr der Teilmatrix M_n' eine ausreduzierte Matrix $\dot{M}_n$ entspricht,[33] weshalb nach dem Hauptsatz die Anzahl der Diagonalelemente 1 von M_n' notwendig gleich e_{n+1} ist.

Da nunmehr die ersten e_{n+1} Spalten von $M(n)$ aus lauter Elementen 1 bestehen und die Klassen (52) die Gruppe $\mathfrak{A}_1$ erzeugen, so gilt

$$\left(\frac{K_n^{(i)}}{A}\right) = 1 \qquad (i = 1, \ldots, e_{n+1};\ A \in \mathfrak{A}_1).$$

Hieraus folgt nach Satz 3, daß es über den Körpern

(61) $$K_n^{(1)}, \ldots, K_n^{(e_{n+1})}$$

je einen Körper

(62) $$K_{n+1}^{(1)}, \ldots, K_{n+1}^{(e_n+1)}$$

gibt. Wird in (53) das Teilsystem (61) durch (62) ersetzt, so bilden (52), (53) offenbar ein $n+1$-stufiges System; ferner ist klar, daß die zugehörige Matrix $M(n+1)$ den oben gestellten Anforderungen genügt. Da dabei (62) sich aus (61) durch e_{n+1} elementare Körperkonstruktionen gewinnen läßt und sonst wir während unseres Verfahrens zu keinen weiteren Körperkonstruktionen zu greifen genötigt sind,[34] so verläuft alles nach Wunsch.

(Eingegangen am 10. Juli 1953.)

Literaturverzeichnis

[1] H. Hasse, Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, Teil I, Ia, II. *Jahresbericht d. D. M. V.*, **35** (1926), S. 1—55; **36** (1927), S. 233—311; Ergänzungsband **6** (1930), S. 1—204.

[2] H Hasse, *Vorlesungen über Zahlentheorie* (Berlin, 1950).

[3] S. Kuroda, Über die Zerlegung rationaler Primzahlen in gewissen nicht-abelschen galoisschen Körpern, *Journ. of the Math. Soc. of Japan*, **3** (1951), S. 150—156.

[4] L. Rédei, Ein neues zahlentheoretisches Symbol mit Anwendung auf die Theorie der quadratischen Zahlkörper, *Journ. f. reine u. angew. Math.*, **180** (1938), S. 1—43.

[5] L. Rédei, Über die Klassengruppen und Klassenkörper algebraischer Zahlkörper, *Journ. f. reine u. angew. Math.*, **186** (1944), S. 80—90.

[33] Darauf haben wir eben angespielt, als wir oben gesagt haben, daß die zweite Reduktion von $M(n)$ im wesentlichen mit dem Ausreduzieren von M_n übereinstimmt.

[34] Die Anwendung von Hilfssatz 2 erfordert nur die sogenannten Körperoperationen, worunter wir die Bildung des Produktes und der Unterkörper von bekannten Körpern verstehen.

[6] L. Rédei, Die Primfaktoren der Zahlenfolge 1, 3, 4, 7, 11, 18, ..., *Portugaliae Mathematica*, **8** (1949), S. 59—61.
[7] L. Rédei, Quadratische Zahlkörper und Theorie der Pellschen Gleichung, *Acta Math. Acad. Sci. Hung.*, **4** (1953), S. 31—87 (die nachstehende Arbeit).
[8] H. Reichardt, Zur Struktur der absoluten Idealklassengruppe im quadratischen Zahlkörper, *Journ. f. reine u. angew. Math.*, **170** (1933), S. 75—82,

ПРИМЕНЕНИЕ УСЛОВНЫХ СИМВОЛОВ АРТИНА В ТЕОРИИ ПОЛЕЙ КЛАССОВ

Л. РЭДЭИ (Сегед)

(Резюме)

Пусть Ω — алгебраическое поле конечного порядка, H — группа идеалов Вебера—Такаги в нём, $\mathfrak{H}$ — соответствующая группа классов (в которой H главный класс). Не уменьшяя существенно общности, можно предположить, что порядок группы $\mathfrak{H}$ есть степень некоторого простого числа l. Обозначим через Ω_H поле классов от Ω, относящееся к H. Тогда (относительный) порядок (относительного) поля $\Omega_H|\Omega$ есть степень числа l. Обозначим через K_n $(n=0, 1, \ldots)$ (относительное) циклическое подполе порядка l^n от Ω_H Ω (в частности $K_0=\Omega$). Вместо K_1 будем просто писать K. Обозначим через C любой элемент группы $\mathfrak{H}$.

Определение. Пусть K, C, n $(n\geqq 1)$ выбраны так, что над K существует хотя бы одно K_n и что порядок символа Артина[1]

$$\left(\frac{K_n}{C}\right) \qquad (K_n \supseteq K) \tag{3}$$

является инвариантом и $\leqq l$. Тогда мы говорим, что существует условный символ Артина

$$\left(\frac{K}{C}\right)_n \tag{4}$$

и договариваемся в том, что

$$\left(\frac{K}{C}\right)_n = 1 \quad \text{или} \quad \left(\frac{K}{C}\right)_n = -1, \tag{5}$$

в зависимости от того, что (общий) порядок символов (3) равен 1 или l. Число n называем индексом символа (4).

Конечно, $\left(\frac{K}{C}\right)_1$ всегда существует и равен 1 или -1 в зависимости от того, является ли $\left(\frac{K}{C}\right)$ идентичным отображением или нет.

Из известных свойтсв символа Артина без особого труда могут быть выведены некоторые свойства условного символа Артина, из которых мы упомянём здесь лишь следующие два свойства:

[1] Под символом (3) понимаем символ Артина

$$\left(\frac{K_n}{\mathfrak{a}}\right) = \left(\frac{K_n|\Omega}{\mathfrak{a}}\right),$$

где $\mathfrak{a}$ является любым идеалам из класса C. Так как по теореме взаимности Артина символы $\left(\frac{K_n}{\mathfrak{a}}\right)$ равны для всех идеалов $\mathfrak{a}(\in C)$, то это „инвариантное обозначение“ (3) символов Артина законно. Соответственно мы будем обозначать и следующие выше условные символы Артина „инвариантным способом“.

Теорема 1. (Правило умножения условного символа Артина по знаменителю.) Если для данного числа n $(n \geqq 1)$, поля K и различных классов C и C' среди $l+1$ условных символов Артина

(9) $$\left(\frac{K}{C''}\right)_n \qquad (C''=C, C', CC', C^2C', \ldots, C^{l-1}C')$$

хотя бы два существуют, то все они существуют и либо все равны 1, либо единственный средних равен 1.

Теорема 2. (Правило умножения условного символа Артина по числителю.) Если для данного числа n $(n \geqq 1)$, класса C и полей K и K' среди $l+1$ условных символов Артина

(10) $$\left(\frac{K''}{C}\right)_n \qquad (\Omega \subset K' \subset KK')$$

существует хотя бы два, то все они существуют и либо все равны 1, либо единственный из них равен 1.

Рассмотрим, вообще, какую-либо прямоугольную матрицу, составленную из символов (4)

(11) $$M=\begin{pmatrix} \left(\frac{K^{(1)}}{C^{(1)}}\right)_n & \left(\frac{K^{(2)}}{C^{(1)}}\right)_n & \cdots \\ \left(\frac{K^{(1)}}{C^{(2)}}\right)_n & \left(\frac{K^{(2)}}{C^{(2)}}\right)_n & \cdots \\ \vdots & & \end{pmatrix}$$

которая, таким образом, (кроме n) является функцией (конечного числа) переменных

(12) $$C^{(1)},\ C^{(2)}, \ldots,$$

(13) $$K^{(1)},\ K^{(2)}, \ldots,$$

и предположим, что поля независимы (13) (над основным полем Ω). Назовём матрицу M приведённой, если значение всех элементов вне диагонали равно 1 и на диагонали элементы 1 стоят перед элементами -1. Под элементарным преобразованием матрицы M понимаем замену класса $C^{(s)}$ каким-либо классом $C = (C^{(r)})^i C^{(s)}$ $(r \neq s;\ i=0,\ldots,l-1)$ или $K^{(s)}$ каким-либо полем $K \subset K^{(r)}K^{(s)}$, $\neq K$ $(r \neq s)$. Из теорем 1 и 2 следует, что матрицу M можно свести к приведённой при помощи элементарных преобразований и перемещений столбцов и строк. Если после приведения матрицы мы вычеркнем все те столбцы и строки, которые содержат элементы -1 и увеличим в оставшейся матрице индекс n элементов до $n+1$, то снова получим матрицу вида (11), которую мы назовём производной матрицы M. Конечно, в общем случае, она неединственна и её элементы не всегда существуют.

Пусть, в частности, $n=1$ и предположим, что классы (12) являются одной из производящих систем подгруппы, образованной элементами порядка $\leq l$ группы $\mathfrak{H}$, и, что поля (13) независимы и их произведение содержит все K. Пусть M_1 обозначает такую специальную матрицу.

Основная теорема. Можно образовать последовательность

(15) $$M_1, M_2, \ldots, M_\nu.$$

в которой M_{i+1} есть производная от M_i $(i=1,\ldots,\nu-1)$ так, что каждая M_i $(i=1,2,\ldots,\nu)$ состоит из существующих элементов и (любая) производная от M_ν есть пустая матрица. Число ν и число столбцов каждой M_i являются инвариантами, а именно: l^ν является максимумом инвариантов (абелевой) группы $\mathfrak{H}$ и число столбцов M_i равняется числу инвариантов группы $\mathfrak{H}$, делящихся на l^i.

Таким образом, эта основная теорема даёт хорошо обозримый („инвариантный“) метод для определения структуры, т. е. инвариантов группы классов $\mathfrak{H}$.

DIE 2-RINGKLASSENGRUPPE DES QUADRATISCHEN ZAHLKÖRPERS UND DIE THEORIE DER PELLSCHEN GLEICHUNG

Von

LADISLAUS RÉDEI (Szeged), korrespondierendem Mitglied der Akademie

Herrn Professor Helmuth Hasse hochachtungsvoll zugeeignet

Definitionen und durchgängige Bezeichnungen:

P der rationale Zahlkörper.

[P] der Ring der ganzen rationalen Zahlen. Die in der Restklasse 1 (mod 4) enthaltenen Elemente von [P] werden primäre Zahlen, die von 1 verschiedenen quadratfreien primären Zahlen und die 4-fachen der quadratfreien nichtprimären Zahlen werden Diskriminantenzahlen genannt. (Diese fallen mit den Diskriminanten der quadratischen Zahlkörper zusammen.) Die nur durch eine Primzahl teilbaren Diskriminantenzahlen nennen wir kurz Stammdiskriminanten. Diese sind die primären Primzahlen und -4, 8, -8. Jede Diskriminantenzahl läßt sich in ein Produkt von Stammdiskriminanten zerlegen. Die Faktoren sind abgesehen von der Reihenfolge eindeutig bestimmt, sie werden die Stammdiskriminantenfaktoren der betrachteten Diskriminantenzahl genannt.

$x, x', x'', y, y', y'', z$ irgendwelche Elemente von [P].

Ω ein beliebig gegebener quadratischer Zahlkörper.

$[\Omega]$ der Ring der ganzen Elemente von Ω.

d das eindeutig bestimmte quadratfreie Element von [P] mit $\Omega = \mathrm{P}(\sqrt{d})$.

D die Diskriminante von Ω, also $D = d$ oder $4d$, je nachdem d primär oder nichtprimär ist. Entsprechend besteht $[\Omega]$ aus den Elementen $\frac{1}{2}(x + y\sqrt{d})$ $(2 \mid x - y)$ bzw. $x + y\sqrt{d}$.

D-Zerfällung bedeutet ein (geordnetes) Paar von zwei ganzen rationalen Zahlen mit dem Produkt D, die entweder beide Diskriminantenzahlen sind, oder die eine von ihnen gleich 1 (die andere gleich D) ist. Diesen zwei Fällen entsprechend nennen wir die *D*-Zerfällung echt

bzw. unecht. Es gibt also genau zwei unechte D-Zerfällungen, nämlich $1, D$ und $D, 1$.

d', d'' ein (geordnetes) Paar von zwei rationalen Zahlen, so daß $d'>0$ ist, ferner entweder d', d'' ganze Zahlen sind mit $d'd''=d$, oder $d\equiv 3 \pmod 4$ ist, $2d', 2d''$ ungerade ganze Zahlen sind mit $d'd''=\frac{1}{4}d$.

m eine zu D prime quadratfreie ungerade natürliche Zahl,[1] die wir bequemlichkeitshalber als primär annehmen.

m', m'' ein (geordnetes) Paar von primären Zahlen mit $m'm''=m$.

t die Anzahl der verschiedenen Primfaktoren von Dm.

$\mathfrak{S}=(d', d'', m', m'')$, $\mathfrak{S}^*=(d'', d', m'', m')$ (keine Ideale oder größten gemeinsamen Teiler!) das (geordnete) System der Zahlen d', d'', m', m'' bzw. d'', d', m'', m'. Die Anzahl der $\mathfrak{S}$ und auch die der $\mathfrak{S}^*$ ist leicht ersichtlich gleich 2^t. Im Fall $d>0$ ist auch $d''>0$, somit stimmen dann die $\mathfrak{S}^*$ (in anderer Reihenfolge) mit den $\mathfrak{S}$ überein. Im Fall $d<0$ sind die $\mathfrak{S}^*$ von den $\mathfrak{S}$ verschieden. Insbesondere:

$\mathfrak{S}_1=(1, d, 1, m)$, $\mathfrak{S}_1^*=(d, 1, m, 1)$. (Die übrigen $\mathfrak{S}^*$ werden nicht in Betracht kommen.)

$\mathfrak{S}$ die (multiplikative) Gruppe aller Systeme $\mathfrak{S}$, wobei wir unter dem Produkt $\mathfrak{S}^{(1)}\mathfrak{S}^{(2)}$ von zwei Systemen $\mathfrak{S}^{(i)}=(d_i', d_i'', m_i', m_i'')$ $(i=1,2)$ dasjenige System $\mathfrak{S}=(d', d'', m', m'')$ verstehen, wofür $d_1'd_2'd', m_1'm_2'm'$ Quadratzahlen in P sind. Man macht sich leicht klar, daß diese Definition korrekt ist. Man sieht auch, daß $\mathfrak{S}$ kommutativ ist und $\mathfrak{S}_1$ zum Einselement hat. Es gelten noch $O(\mathfrak{S})=2^t$, $\mathfrak{S}^2=\mathfrak{S}_1$:

p_∞ die (einzige) unendliche Primstelle von P.[2]

$[\Omega]_m$ der Unterring von $[\Omega]$ bestehend aus denjenigen Elementen von $[\Omega]$, die einer (ganzen) rationalen Zahl $\bmod m$ kongruent sind. Kurz nennen wir $[\Omega]_m$ den Ring $\bmod m$, seine Elemente die Ringzahlen $\bmod m$ und die Einheiten in $[\Omega]_m$ die Ringeinheiten $\bmod m$. Insbesondere ist $[\Omega]_1=[\Omega]$. Entsprechend sind also die Ringzahlen und Ringeinheiten mod 1 einfach die ganzen Zahlen bzw. die Einheiten in Ω.

$[\Omega]^{(g)}$ der Unterring von $[\Omega]$ bestehend aus den Zahlen $x+y\sqrt{d}$. (In der Bezeichnung $[\Omega]^{(g)}$ läßt uns „(g)“ daran erinnern, daß die

[1] Der Fall $2|m$ würde für einen Teil unserer Untersuchungen beträchtliche Verwicklungen machen, weshalb wir davon absehen wollten. Dagegen werden die Annahmen, daß m zu d prim und quadratfrei ist, die Allgemeinheit unserer Untersuchungen nicht einschränken (vgl. [4]). Alle die oben noch folgenden „durchgängigen“ Bezeichnungen beziehen sich auf aus den für die ganze Arbeit festzuhaltenden zwei Angaben Ω, m (oder d, m) abzuleitende Begriffe. Man bemerke, daß d jede quadratfreie ganze rationale Zahl $\neq 1$ sein kann.

[2] Bezüglich der Grundbegriffe und Hauptsätze der Klassenkörpertheorie, sowie der in dieser üblichen Terminologie und Bezeichnungsart verweisen wir ein für allemal auf die Arbeiten von HASSE [3]. (Mit [ ] verweisen wir auf das Literaturverzeichnis am Schluß unserer Arbeit.)

„Koordinaten" x, y der Elemente von $[\Omega]^{(g)}$ ganz sind.) Es gilt $[\Omega]^{(g)} = [\Omega]$ dann und nur dann, wenn $2|D$ ist.

$[\Omega]_m^{(g)} = [\Omega]_m \cap [\Omega]^{(g)}$. Wieder gilt $[\Omega]_m^{(g)} = [\Omega]_m$ dann und nur dann, wenn $2|D$ ist.

$\tilde{m} = m p_\gamma$.

H_m die (multiplikative) Gruppe derjenigen zu $\tilde{m}$ primen Zahlen $\alpha (\in \Omega)$, für die

$$\alpha \equiv r \pmod{\tilde{m}}$$

mit einem $r (\in P)$ lösbar ist.[3] Wir fassen die Zahlgruppe $H_{\tilde{m}}$ auch als Idealgruppe auf, nämlich als die Gruppe der durch die gesagten α erzeugten Hauptideale (α). Sonst auch werden wir oft eine algebraische Zahl ω auch als das durch sie erzeugte Hauptideal (ω) auffassen und auch hierfür einfach ω schreiben, ein Mißverständnis wird daraus nicht entstehen.

H die Gruppe derjenigen (ganzen und gebrochenen) Ideale in Ω, von denen eine ungerade Potenz in $H_{\tilde{m}}$ fällt. Es ist klar, daß H eine mod $\tilde{m}$ erklärbare Idealgruppe von Ω ist im Sinne von WEBER—TAKAGI.

§ 1. Probleme I bis IV

Es wird sich in dieser Arbeit um die vollständige Beantwortung von vier Problemen I bis IV handeln. Bevor wir sie formulieren, bemerken wir, daß die Klassenzahl von Ω nach H offenbar die Potenz von 2 ist, somit sind für Ω und H die Voraussetzungen unserer vorstehenden Arbeit [8] mit $l = 2$ erfüllt. Deshalb dürfen und wollen wir die vorliegende Arbeit als eine Fortsetzung von [8] für diese speziellen Ω und H ansehen. Entsprechend übernehmen wir aus [8] alle die dort an die Spitze gestellten „durchgängigen" Bezeichnungen, alles stillschweigend auf die obigen Ω, H (und $l = 2$) bezogen. Also ist jetzt insbesondere $\mathfrak{H}$ eine 2-Klassengruppe, die wir die 2-Ringklassengruppe mod $\tilde{m}$ von Ω nennen, ferner ist jetzt e_n die Anzahl der durch 2^n teilbaren Invarianten von $\mathfrak{H}$.[4] (Im Spezialfall $m = 1$ ist $\mathfrak{H}$ die sogenannte abso-

[3] Natürlich ist obige Kongruenz im multiplikativen Sinne zu verstehen.

[4] Selbst die Klassengruppe nach $H_{\tilde{m}}$ pflegt man die im engeren Sinne genommene (volle) Ringklassengruppe mod m von Ω zu nennen. Es bedeutet e_n auch die Anzahl der durch 2^n teilbaren Invarianten von dieser Ringklassengruppe, da diese dieselben geraden Invarianten hat wie $\mathfrak{H}$. — Hier wollen wir kurz auseinandersetzen, warum wir ohne Einschränkung der Allgemeinheit nur die zu d primen, quadratfreien m in Betracht ziehen. Bezeichne a eine primäre Zahl, deren Primfaktoren lauter Teiler von dm sind. Da $2 \nmid m$ ist, so folgt aus der Kongruenz $\alpha \equiv r \pmod{\tilde{m}}$ in der Definition von $H_{\tilde{m}}$ offenbar $\alpha^{|a|} \equiv r^{|a|} \pmod{a\tilde{m}}$. Hieraus und aus der Definition von H sieht man, daß (selbst $H_{\tilde{m}}$ noch nicht aber) H, also auch $\mathfrak{H}$ und somit Problem I gegenüber der Ersetzung $m \to a m$ invariant ist. Zerlegen wir ferner a in das Produkt $a' a''$ von zwei primären Zahlen a', a'', für die

lute 2-Klassengruppe von Ω im engeren Sinne.) Den H zugeordneten Klassenkörper Ω_H können wir jetzt den vollen 2-Ringklassenkörper mod $\tilde{m}$ (von Ω), die Unterkörper von Ω_H kurz die Ringklassenkörper (von Ω) nennen.

Problem I bestehe für jedes Paar[5] d, m in der Bestimmung (von ν und) der Zahlen

$$e_1 \geqq \cdots \geqq e_\nu > e_{\nu+1} = 0, \tag{1}$$

d. h. in der Erforschung der Struktur der 2-Ringklassengruppe $\mathfrak{H}$ mod $\tilde{m}$ des quadratischen Zahlkörpers Ω.

Problem II bestehe für jedes n $(=1, 2, \ldots)$ und jedes System $\mathfrak{S} = (d', d'', m', m'')$ in der Untersuchung der Diophantischen Gleichung

$$d' m'^2 x'^2 - d'' m''^2 x''^2 = z^{2^n} \qquad ((m'x', m''x'', z) = 1; 2 \nmid z) \tag{2}$$

nach Lösbarkeit.[6]

Problem III bestehe für jedes System $\mathfrak{S} = (d', d'', m', m'')$ in der Untersuchung der Dirichletschen Gleichung[7]

$$d' m'^2 x'^2 - d'' m''^2 x''^2 = 1 \tag{3}$$

nach Lösbarkeit.[8]

Problem IV bestehe für jedes Paar d, m in der Untersuchung der („negativen") Pellschen Gleichung[9]

$$x^2 - d m^2 y^2 = -1 \tag{4}$$

nach Lösbarkeit.[10]

$(a', d'' m'') = (a'', d' m') = 1$ ist. Nehme man dann eine Lösung von (2), bilde aus ihr die Zahl $m' x' \sqrt{d'} + m'' x'' \sqrt{d''}$. Wird diese zur $|a|$-ten Potenz erhoben, so entsteht offenbar eine Zahl von der Form $a' m' y' \sqrt{d'} + a'' m'' y'' \sqrt{d''}$ mit $(a' m' y', a'' m'' y'') = 1$. Hieraus sieht man leicht ein, daß durch die Ersetzung $m \to am$ auch Problem II nicht beeinflußt wird. Ähnliches gilt über Problem III und offenbar auch über Problem IV.

[5] D. h. für jedes Paar Ω, H. Die Paare Ω, H und d, m bestimmen nämlich einander eindeutig.

[6] Nach der Definition der Zahlen d', d'', m', m'' sind die Koeffizienten in (2) entweder ganz oder sie haben den Nenner 2. Im letzteren Fall könnte man mit 2 heraufmultiplizieren, damit man zu ganzen Koeffizienten kommt, für uns wird aber die obige Form der Gleichungen (2) bequemer. Ähnliches bezieht sich auch auf die Gleichungen (3). In beiden Gleichungen (2), (3) achten wir stets auch auf die Reihenfolge der Glieder. Für $n = 1$ ist (2) ein Spezialfall der wohlbekannten Lagrangeschen Gleichung $ax^2 + by^2 + cz^2 = 0$.

[7] Vgl. Dirichlet [1].

[8] Man bemerke, daß für den Fall $\mathfrak{S} = \mathfrak{S}_1 = (1, d, 1, m)$ sowohl (2) (für jedes n) als auch (3) lösbar ist. Hiernach genügte es, sich in den Problemen II, III auf die $\mathfrak{S} \neq \mathfrak{S}_1$ zu beschränken. Man dürfte sich ferner im Problem III auf die $d > 0$ beschränken. Es wird aber bequemer, beide Probleme in obiger Allgemeinheit ins Auge zu fassen.

[9] Der scheinbar allgemeinere Fall $x^2 - dm^2y^2 = -4$ läßt sich bekanntlich auf (4) zurückführen (s. [10]). Natürlich kann (4) im Fall $d < 0$ nicht lösbar sein, trotzdem wollen wir bequemlichkeitshalber die $d < 0$ auch im Problem IV zulassen. Schreibt man (4) in der Form $dm^2y^2 - x^2 = 1$, so merkt man, daß es sich um den Spezialfall $\mathfrak{S} = \mathfrak{S}_1^* = (d, 1, m, 1)$

Auch die Probleme II bis IV haben eine körpertheoretische Bedeutung. Und zwar handelt es sich im Problem IV um die Frage der Existenz einer Ringeinheit mod m in Ω mit negativer Norm, ferner werden wir im § 4 sehen, daß Problem II und Problem III der Bestimmung der Gruppen $\mathfrak{A}_n$ bzw. der Gruppe $\mathfrak{A}_1$ gleichkommt.

Es wäre schwer unsere Probleme I bis IV nach ihrer Wichtigkeit zu ordnen, da sie miteinander in sehr nahem Zusammenhang stehen. Noch mehr werden sie dadurch einander nahe gebracht, daß ihre Lösung in *einer* Theorie entstehen wird. Genauer gesprochen, gleichzeitig mit der Lösung von Problem I werden auch schon die Probleme II bis IV mitbeantwortet, und es gilt auch die Umkehrung, daß keins der letzteren Probleme ohne Problem I allgemein [11] gelöst werden kann, weshalb es sich im wesentlichen um vier (innerhalb unserer Theorie) äquivalente Probleme handelt.

In der historischen Entwicklung sind die Probleme I bis IV in der Reihenfolge IV, I, III, II aufgetaucht worden (s. § 2). Diese, oder vielleicht mit mehr Recht I, IV, III, II könnte man für ihre Wichtigkeitsreihenfolge hinnehmen. Die von uns gewählte Reihenfolge I, II, III, IV spiegelt mehr den logischen Zusammenhang unserer Probleme. Ohne Zweifel hat man nämlich die Untersuchungen mit Problem I anzufangen, wie wir es auch tun werden, und man wird sehen, wie mit der Lösung von Problem I zusammen die Probleme II, III, IV in *dieser* Reihenfolge ohne Zwang mitgelöst werden.

von (3) handelt. Hiernach ist Problem IV ein Teil von Problem III. Offenbar kann (4) nur dann lösbar sein, wenn $d > 0$ ist und dm^2 keinen positiven Primfaktor von der Form $4k+3$ enthält. In diesem Fall pflegt man dm^2 (im Zusammenhang mit (4)) eine *kritische Zahl* zu nennen. Wir dürfen uns im Problem IV stets auf die kritischen Zahlen beschränken, aber meistens wird diese Annahme überflüssig.

[10] Bis auf Problem IV sind bekanntlich alle Grundfragen der Theorie der Pellschen Gleichung in befriedigender Weise schon längst erledigt worden. Mit Problem IV ist es anders. Wohl entscheidet nämlich das bekannte Kettenbruchkriterium dem Wortlaut nach sehr einfach über die Lösbarkeit von (4), nach dem nämlich (4) dann und nur dann lösbar ist, wenn ($d > 0$ und) die kleinste Periodenlänge der regulären Kettenbruchentwicklung von $m\sqrt{d}$ eine ungerade Zahl ist, aber dieses Kriterium ist in mehrerer Hinsicht unbefriedigend und gilt mehr für ein Aufschieben als eine Lösung des Problems. (Von der sonst sehr interessanten elementaren Methode von Epstein [2] ist eine befriedigende Lösung des Problems IV auch nicht zu erwarten. Vgl. auch Rédei [14].) Zum Beispiel weiß man nämlich andererseits schon seit Lagrange, daß $x^2 - py^2 = -1$ (p Primzahl, > 0) dann und nur dann lösbar ist, wenn $p \not\equiv 3 \pmod 4$ gilt. Um diesen Satz zu beweisen, ist das Kettenbruchkriterium völlig unbrauchbar. Die von uns beabsichtigte Lösung von Problem IV wird als Spezialfall den Satz von Lagrange und überhaupt alle bekannten, gut brauchbaren, teils hinreichenden teils notwendigen, aber bisher sehr lückenhaften Bedingungen für die Lösbarkeit von (4) in sich enthalten und diese zu einem vollständigen Kriterium ausbauen, weshalb wir sagen können, daß wir in dieser Arbeit die Theorie der Pellschen Gleichung zu einem langersehnten Abschluß bringen werden.

[11] In Spezialfällen kann Problem IV ohne die vollständige Lösung von Problem I gelöst werden, worüber wir unten näheres sagen.

Gleich hier wollen wir etwas näher besprechen, wie sich die Lösung unserer Probleme I bis IV gestaltet, bezüglich der Einzelheiten verweisen wir auf §§ 3, 4 (Sätze 1 bis 4).

Über Problem I bemerken wir, daß dieses ein verhältnismäßig leichter Spezialfall des im Hauptsatz unserer Arbeit [8] allgemein gelösten Problems ist. Entsprechend werden wir Problem I als unmittelbare Anwendung des genannten Hauptsatzes lösen, die trotzdem keine „mechanische“, sondern eine lehrreiche Anwendung sein wird. Und zwar werden wir vor allem eine Basis

$$K^{(1)}, \ldots, K^{(t-1)} \tag{5}$$

der Körpermenge $\mathfrak{M}_1$ bestimmen (womit wir zugleich auch schon den e_1-Schritt unseres in [8] § 3 beschriebenen Algorithmus ausgeführt werden haben). Aus der Basiseigenschaft von (5) folgt nach [8] (17) (s. dort auch Lemma 1)

$$e_1 = t-1. \tag{6}$$

Wieder nach [8] (17) gilt also

$$O(\mathfrak{A}_1) = 2^{t-1}, \tag{7}$$

folglich besteht eine Basis der Gruppe $\mathfrak{A}_1$ aus $t-1$ Elementen. Es liegt nun an der Natur, daß man nicht leicht sofort auch eine Basis von $\mathfrak{A}_1$ aufstellen kann, sondern wird das erst durch die Lösung von Problem III ermöglicht (s. unten). Zum Glück ist aber die Lösung von Problem I auch ohne die Kenntnis einer Basis von $\mathfrak{A}_1$ möglich, es genügt ja, wenn man ein System erzeugender Elemente von $\mathfrak{A}_1$ aufstellt. Das geht so. Es wird sich ein Homomorphismus

$$\mathfrak{S} \sim \mathfrak{A}_1 \quad (\mathfrak{s} \rightarrow A(\mathfrak{s})) \tag{8}$$

angeben lassen, wobei wir mit $A(\mathfrak{s})$ das homomorphe Bild von $\mathfrak{s}$ bezeichnen. Da wir andererseits leicht eine Basis

$$\mathfrak{s}^{(1)}, \ldots, \mathfrak{s}^{(t)} \tag{9}$$

von $\mathfrak{S}$ angeben werden können, so wird uns hierdurch wegen (8) auch schon ein System

$$A(\mathfrak{s}^{(1)}), \ldots, A(\mathfrak{s}^{(t)}) \tag{10}$$

erzeugender Elemente von $\mathfrak{A}_1$ zur Verfügung stehen. Aus (5) und (10) bilden wir dann die Matrix

$$M_1 = \begin{vmatrix} \left(\frac{K^{(1)}}{A(\mathfrak{s}^{(1)})}\right)_1 & \cdots & \left(\frac{K^{(t-1)}}{A(\mathfrak{s}^{(1)})}\right)_1 \\ \vdots & & \vdots \\ \left(\frac{K^{(1)}}{A(\mathfrak{s}^{(t)})}\right)_1 & \cdots & \left(\frac{K^{(t-1)}}{A(\mathfrak{s}^{(t)})}\right)_1 \end{vmatrix} \tag{11}$$

vom Typ $t \times (t-1) \, (= (e_2+1) \times e_2)$. Man hat dann nur noch von M_1 ausgehend eine Folge

$$M_1, M_2, \ldots \tag{12}$$

von höheren Ableitungen nach der Vorschrift in [8] § 2 aufzustellen, womit wir also Problem I als gelöst ansehen können. Und zwar bestimmt sich e_n $(n=1,\ldots,\nu)$ allgemein als die Anzahl der Spalten von M_n, ferner wird ν als der Index des letzten nichtverschwindenden Gliedes der Folge (12) kenntlich. (Kurz gesprochen, man hat unseren in [8] § 3 beschriebenen Algorithmus an (11) beginnend auszuführen. Die Ausführung der e_1-, ..., e_n-Schritte dieses Algorithmus setzt uns eben in die Kenntnis von e_n.)

Bezüglich der Lösung von Problem II bemerken wir, daß man es bei festgehaltenen d, m, n mit genau 2^t Gleichungen (2) zu tun hat. Wir bezeichnen mit $\mathfrak{S}_n$ die Menge derjenigen Systeme $\mathfrak{s}$, für die die Gleichung (2) lösbar ist. Dann läuft Problem II auf die Bestimmung von $\mathfrak{S}_n$ hinaus. Nach gilt $\mathfrak{s}_1 \in \mathfrak{S}_n$. Wir werden ferner leicht zeigen, daß $\mathfrak{S}_n$ eine Gruppe ist mit

$$O(\mathfrak{S}_n) = 2^{1+e_n}. \tag{13}$$

Ein Blick auf (2) macht auch klar, daß $\mathfrak{S}_1 \supseteqq \mathfrak{S}_2 \supseteqq \cdots$ gelten muß. Dies mit (1), (13) zusammen ergibt sogar

$$\mathfrak{S}_1 \supsetneqq \cdots \supsetneqq \mathfrak{S}_{\nu-1} \supset \mathfrak{S}_\nu = \mathfrak{S}_{\nu+1} = \cdots \tag{14}$$

Es wird sich nun herausstellen, daß die Lösung von Problem I auch schon die von Problem II liefert, und zwar durch die Ausführung des e_{n+1}-Schrittes unseres Algorithmus wird die Gruppe $\mathfrak{S}_n$ bekannt. (Des näheren: die in der Matrix M_{n+1} vorkommenden Nenner erscheinen in der Form $A(\mathfrak{s})$, wobei die $\mathfrak{s}$ eben eine Basis von $\mathfrak{S}_n$ durchlaufen, andererseits werden diese $A(\mathfrak{s})$ schon durch den e_{n+1}-Schritt des Algorithmus kenntlich.)

Bezüglich der Lösung von Problem III bemerken wir, daß man es bei festen d, m ebenfalls mit genau 2^t Gleichungen (3) zu tun hat. Unter diesen gibt es — wie wir es leicht sehen werden — genau zwei lösbare. Die eine von diesen gehört nach[8] zu $\mathfrak{s}_1$. Wir bezeichnen mit $\mathfrak{s}_\infty$ dasjenige System, dem die andere der gesagten Gleichungen angehört. Dann hat man zur Lösung von Problem III nur $\mathfrak{s}_\infty$ zu bestimmen. Andererseits zeigt ein Blick auf (2) und (3), das $\mathfrak{s}_\infty$ in allen $\mathfrak{S}_n$ enthalten sein muß. (Aus diesem Grunde haben wir die Bezeichnung $\mathfrak{s}_\infty$ eingeführt.) Da ferner durch die Lösung von Problem II insbesondere $\mathfrak{S}_\nu$ bestimmt wird, so wird hierdurch wegen $O(\mathfrak{S}_\nu) = 2$ auch schon $\mathfrak{s}_\infty$ bekannt, als das von $\mathfrak{s}_1$ verschiedene Element von $\mathfrak{S}_\nu$.

Bezüglich der Lösung von Problem IV bemerken wir, daß sich die Gleichung (4) in der Form $dm^2y^2 - x^2 = 1$ schreiben läßt, woraus man sieht, daß (4) im Fall $d>0$ mit dem zum System $\mathfrak{s}_1^* = (d, 1, m, 1)$ gehörenden Fall von (3) übereinstimmt. Hiernach ist (4) dann und nur dann lösbar, wenn $\mathfrak{s}_\infty = \mathfrak{s}_1^*$ gilt. (Darin ist die Bedingung $d>0$ schon mitenthalten.)

Kurze Zusammenfassung. Indem man unseren Algorithmus ausführt, werden nach und nach die Zahlen $e_1, \ldots, e_\nu (>0), e_{\nu+1} (=0)$ und die Untergruppen $\mathfrak{S}_1, \ldots, \mathfrak{S}_\nu$, ferner mit $\mathfrak{S}_\nu$ zusammen das System $\mathfrak{s}_\infty$ bekannt und

hierdurch insbesondere auch entschieden, ob $\mathfrak{S}_\infty = \mathfrak{S}_1^*$ gilt. Dies alles bedeutet der Reihe nach die Beantwortung der Probleme I bis IV.

Man sieht aus dem Gesagten, daß — wie auch schon oben bemerkt wurde — in unseren Untersuchungen die Probleme I bis IV äquivalent sind, denn im allgemeinen wird keins ohne das andere vollständig gelöst. Dagegen trifft das *in Spezialfällen* für Problem IV nicht immer zu, was wir schon in[11] bemerkt haben und hier genau besprechen wollen. Fassen wir hierzu ein beliebiges aber festes Paar d, m ins Auge. Wir unterscheiden zwei Fälle. *Erstens* sei die Pellsche Gleichung (4) lösbar, d. h. $\mathfrak{S}_\infty = \mathfrak{S}_1^*$, was man auch in der Form $\mathfrak{S}_1^* \in \mathfrak{Z}_\nu$ ausdrücken kann. Diese Tatsache wird durch unseren Algorithmus erst dann bekannt, wenn dieser ganz zu Ende geführt wird. *Zweitens* sei (4) unlösbar, d. h. $\mathfrak{S}_1^* \notin \mathfrak{Z}_\nu$. Ist dabei noch $\mathfrak{S}_1^* \in \mathfrak{E}_{\nu-1}$ (vgl. (12)), so gilt das Gesagte wieder. Ist dagegen sogar $\mathfrak{S}_1^* \notin \mathfrak{E}_{\nu-1}$, so gibt es eine kleinste natürliche Zahl n_0 mit $\mathfrak{S}_1^* \notin \mathfrak{Z}_{n_0} (1 \leqq n_0 \leqq \nu - 1)$, weshalb jetzt schon aus dem e_{n_0+1}-Schritt des Algorithmus die Erkenntnis $\mathfrak{S}_1^* \notin \mathfrak{Z}_\nu$, d. h. die Unlösbarkeit von (4) folgt. Hiernach gilt: wenn die Pellsche Gleichung (4) lösbar ist, so stellt sich das immer erst am Ende unseres Algorithmus heraus, ist sie unlösbar, so kann sich das schon „unterwegs" herausstellen. In unseren Untersuchungen erweist sich also Problem IV für spezielle d, m in der Tat bald mit den Problemen I bis III äquivalent bald diesen Problemen untergeordnet.

Den eben geschilderten merkwürdigen Sachverhalt wollen wir die *Caprice der Pellschen Gleichung* nennen, die nämlich darin besteht, daß für die verschiedenen Paare d, m die Entscheidung über Problem IV im Verhältnis zu Problem I bald eine leichtere bald eine ebenso schwierige Aufgabe ist. Nach obigem haben wir diese Caprice völlig aufgeklärt, aber in den früheren, noch nicht weit genug getriebenen Untersuchungen (s. § 2) schien sich die Pellsche Gleichung (4) im Zusammenhang mit Problem I sehr geheimnisvoll zu benehmen.

Wir wollen betonen, daß nach obigem das Verhalten der Einheiten von Ω vom Verhalten der Klassengruppen in Ω abhängig erscheint.[12] Dieser Abhängigkeit läßt sich die altbekannte Abhängigkeit zwischen Klassengruppe und Einheiten entgegenstellen,[13] die sich in der Klassenzahlformel offenbart, nach der nämlich die Klassenzahl unter anderem von den Einheiten, nämlich vom Regulator abhängig ist.

Zur effektiven Ausführung unseres Algorithmus sind auch gewisse Klassenkörper zu konstruieren (vgl. [8] § 6). Um diese (keine prinzipiellen Schwierigkeiten bietende) Aufgabe zu erleichtern, werden wir nach dem Vorgang von Reichardt [22] die auch an sich interessanten Eigenschaften der

[12] Selbstverständlich, ist ähnliches auch für andere, in [8] vorgelegte Körper Ω zu erwarten.

[13] Diese Gegenüberstellung hat anläßlich meines über das Thema dieser Arbeit im Januar dieses Jahrs an der Universität von Humboldt in Berlin gehaltenen Vortrags Herr H. Reichardt freundlichst bemerkt.

Klassenkörper K_n (für den in dieser Arbeit vorgelegten Fall) näher untersuchen und darauffolgend genaue Anweisungen zu ihrer Konstruktion ausarbeiten. Erst mit diesen Ergänzungen zusammen werden wir dann die Probleme I bis IV als vollständig erledigt ansehen.

Während einerseits unsere Resultate eine völlig abgerundete Theorie bilden, andererseits erhellt ihre Brauchbarkeit aus folgenden wichtigen Anwendungen, mit denen wir uns ein andermal zu beschäftigen beabsichtigen. Zu vorgegebenen ganzen rationalen Zahlen $e_1 \geqq \cdots \geqq e_k (\geqq 0)$ gibt es unendlich viele d, sowohl positive als auch negative, so daß die absolute Klassengruppe (Fall $m = 1$) des zugehörigen $\Omega = \mathrm{P}(\sqrt{d})$ genau e_n durch 2^n teilbare Invarianten hat $(n = 1, \ldots, k)$, auch die asymptotische Verteilung dieser d läßt sich bestimmen. Entsprechendes gilt aber auch für den allgemeinen Fall. Ebenfalls läßt sich das zuerst von NAGELL [6] in Angriff genommene Problem bezüglich der asymptotischen Verteilung der Zahlen dm^2 genau aufklären, für die die Pellsche Gleichung (4) lösbar ist. Weniger scharfe Untersuchungen dieser Art haben wir schon früher [15] gemacht, als wir erst noch über einen kleinen Teil obiger Resultate verfügt haben; die Verschärfung bietet im Besitz vorliegender Arbeit keine ernsten Schwierigkeiten.

Auch soll erwähnt werden, daß man mit Hilfe unserer Resultate ohne sehr große Mühe eine Lösbarkeitstafel der Pellschen Gleichung (4) etwa für die $dm^2 < 10^6$ zusammenstellen kann. Vorarbeiten hierzu liegen mir im Manuskript schon vor. Die umfassendste Tafel dieser Art ist die von PATZ [7], in der (unter anderem) auf Grund des Kettenbruchkriteriums die Fälle $dm^2 < 10^4$ aufgearbeitet wurden.

Wir gliedern unsere Arbeit so:

Im § 2 machen wir im Zusammenhang unserer Probleme einige historische und kritische Bemerkungen, die den Leser von der Zusammengehörigkeit dieser Probleme schon im voraus überzeugen werden.

In den §§ 3, 4 erfolgt die Lösung des Problems I (s. Satz 1) bzw. der Probleme II bis IV (s. Sätze 2 bis 4).

Im § 5 untersuchen wir die Eigenschaften der Klassenkörper K_n (s. Satz 5).

Im § 6 wird die Konstruktion der K_n durchgeführt (s. Satz 6 und seinen Zusatz).

Im § 7 stellen wir einige Teilresultate unserer Untersuchungen zusammen, woraus sichtbar wird, daß unsere Resultate die früheren Forschungen dieser Art umfassen. Hier betrachten wir auch einige Beispiele.[14]

[14] Wir haben zu bemerken, daß wir über den Gegenstand dieser Arbeit schon vor 10 Jahren in ungarischer Sprache eine Arbeit [21] verfaßt haben, die aber wegen des Krieges unvollendet geblieben ist. (Es wurden nämlich vier Mitteilungen geplant, von denen nur drei erschienen sind.) Diese unvollendete Arbeit [21] wird durch die vorliegende sonst auch in mehrerer Hinsicht überholt. Aus diesen Gründen wollen wir auf die Arbeit [21] keine Notiz mehr nehmen und die vorliegende so abfassen, als wenn wir alles erst hier erfunden hätten.

§ 2. Historische und kritische Bemerkungen

Wir wollen kurz über die früheren Untersuchungen bezüglich unserer Probleme I bis IV berichten. Diese betreffen fast ausschließlich den Fall $m=1$, weshalb wir uns hier — wenn nicht anderes gesagt wird — auf diesen Fall beschränken werden. Näher wurden nur die zwei klassischen Probleme I, IV untersucht, entsprechend wird hier meist nur über diese die Rede sein. Unser Hauptzweck ist hier klar zu machen, wie diese scheinbar voneinander weit liegenden Probleme I, IV schon früher miteinander in eine enge Berührung getreten sind und daß deshalb ihre vollständige Lösung nur auf einem gemeinsamen Wege zu erhoffen ist. Hierdurch (und durch den Inhalt vom § 7) wird der Leser überzeugt, daß die in §§ 3, 4 aufzustellenden Sätze eine bestmögliche Lösung unserer Probleme enthalten. Bezüglich näherer historischer Angaben verweisen wir auf die späteren Teile dieser Arbeit und auf das Literaturverzeichnis am Ende dieser Arbeit.

Den ersten Schritt zur Lösung von Problem I hat GAUSS mit seinem berühmten Satz über die Genera (= Geschlechter) der ganzzahligen binären quadratischen Formen getan, nach dem nämlich $e_1 = t-1$ ist.

Bezüglich Problem IV fand DIRICHLET [1] im Zusammenhang mit Problem III gewisse hinreichende Bedingungen, damit (4) lösbar ist. Der erste Teil dieser Bedingungen drückt sich in quadratischen Restsymbolen $\left(\frac{a}{b}\right)$, der zweite in sogenannten rationalen biquadratischen oder Dirichletschen Restsymbolen $\left(\frac{a}{b}\right)_4$ (s. [8] § 1) aus. Nach ihm liegt für

$$x^2-pqy^2=-1 \qquad (p, q \text{ verschiedene Primzahlen}, \equiv 1 \pmod 4))$$

Lösbarkeit vor, wenn entweder

$$\left(\frac{p}{q}\right)=-1$$

oder $\left(\left(\frac{p}{q}\right)=1 \text{ und}\right)$

$$\left(\frac{p}{q}\right)_4=\left(\frac{q}{p}\right)_4=-1$$

gilt. Außer diesem Fall hat DIRICHLET nur noch den Fall

$$x^2-pqry^2=-1 \qquad (p, q, r \text{ verschiedene Primzahlen})$$

betrachtet und fand hierfür zwei ähnliche, etwas kompliziertere Bedingungen. Diese schönen Beispiele wurden lange Zeit nicht genügend gewürdigt, erst TANO [24] hat sie auf den Fall

$$x^2-dy^2=-1 \tag{15}$$

verallgemeinert.

Im Problem I habe ich [9][15] vor zwanzig Jahren mit der Bestimmung von e_2 auf klassenkörpertheoretischem Wege den ersten nennenswerten Fortschritt gemacht, und zwar konnte ich e_2 ebenfalls mit Hilfe von Symbolen $\left(\frac{a}{b}\right)$ ausdrücken. Gleichzeitig machte ich die entscheidende Entdeckung, daß sich der erste Teil der Dirichlet—Tanoschen Bedingungen so aussprechen läßt: *Enthält* $d(>0)$ *keine Primfaktoren von der Form* $4k+3$ *und ist* $e_2=0$, *so ist* (15) *lösbar.* Durch diesen Satz ist Problem IV zum erstenmale mit Problem I in einen Zusammenhang gekommen. Bald nachher machte ich [13] in beiden Problemen I, IV einen weiteren Fortschritt und zog den Zusammenhang zwischen ihnen enger, indem ich e_8 bestimmt und dem zweiten (nämlich durch Symbole $\left(\frac{a}{b}\right)_4$ ausgedrückten) Teil der Dirichlet—Tanoschen (hinreichenden) Bedingungen bezüglich der Lösbarkeit von (15) gewisse ähnlich gebaute aber notwendige Bedingungen an die Seite gestellt, ferner beide dieser Bedingungen wieder mit Problem I in eine Berührung gebracht habe. In den Arbeiten von Inaba [4], Iyanaga [5], Reichardt [22], Scholz [23] und mir [11], [12], [14] bis [18], [20] wurden teils diese ersten Resultate auf mehrere Arten neu bewiesen und vertieft, teils aus ihnen verschiedene Anwendungen gemacht, unter denen insbesondere auch die Lösung vom Problem II für $n=2$ vorkam.

Es war klar, daß es sich in den besprochenen Resultaten um Bruchstücke einer (noch fehlenden) gemeinsamen Theorie der Probleme I bis IV handelt, weshalb ein befriedigender Abschluß der Theorie der Pellschen Gleichung nur darin bestehen kann, daß man die erwähnten teils hinreichenden teils notwendigen Bedingungen für die Lösbarkeit von (4) zu einem die sämtlichen Fälle umfassenden Kriterium vervollkommnet. Hierzu fehlte es aber noch an einem (zahlentheoretischen) Symbol, das zur Beschreibung der Gesetzmäßigkeiten dieser erst aufzustellenden Theorie eignet. Fest hat es nur gestanden, daß dieses Symbol eine Verallgemeinerung des Dirichletschen Symbols $\left(\frac{a}{b}\right)_4$ sein muß, da dieses in den schon entdeckten Gesetzmäßigkeiten eine Rolle gespielt hat. Nach einigem Experimentieren (s. meine Arbeit [17]) fand ich, daß das gesuchte Symbol das in [8] definierte bedingte Artinsche Symbol ist. Mit Hilfe dieses Symbols konnten wir dann den Hauptsatz in [8] aufstellen, auf dem die Lösung unserer Problem I bis IV beruhen wird, wie wir das im § 1 schon besprochen haben. Vgl. noch § 7, wo wir sehen werden, daß das bedingte Artinsche Symbol in der Tat eine Verallgemeinerung von $\left(\frac{a}{b}\right)_4$ ist.

15 Die Arbeit [9] ist unter Mitwirkung von H. Reichardt mit unverändertem Inhalt aber eleganterem Beweis auch in deutscher Sprache erschienen, s. Rédei und Reichardt [10]. Herr H. Hasse hat sich zurzeit über meine ersten Resultate in einem an mich geschriebenen Brief sehr liebevoll geäußert, womit er die Fortsetzung meiner Untersuchungen kräftig befördert hat.

§ 3. Lösung des Problems I

Wir verabreden uns, daß wir mit $\sqrt{d'}$ stets die positive Quadratwurzel von d' bezeichnen. Das bezieht sich auch auf $\sqrt{d}$, insofern d positiv ist. Ferner wählen wir $\sqrt{d''}$ so, daß $\sqrt{d'}\sqrt{d''}$ gleich $\sqrt{d}$ oder $\frac{1}{2}\sqrt{d}$ ist.

Ist ξ eine Zahl in $P(\sqrt{d'}, \sqrt{d''})$, so soll ξ' das Relativkonjugierte von ξ in bezug auf $P(\sqrt{d})$ bezeichnen.[16]

Die Lösung von Problem I ist enthalten im folgenden:

Satz 1. *Um die Körpermenge $\mathfrak{M}_1$ und eine Basis von ihr anzugeben, verfahre man wie folgt. Man wähle einen Primzahlfaktor p von D, der aber im Fall $2|D$ eben $p=2$ sein soll. Durchläuft d_0 die zu p primen und von 1 verschiedenen primären Teiler von dm, so sind die Körper*

$$K = \Omega(\sqrt{d_0}) \tag{16}$$

die sämtlichen verschiedenen Elemente von $\mathfrak{M}_1$. Wenn also $p_1, \ldots, p_{t-1}$ die sämtlichen zu p primen primären Primzahlteiler von dm bezeichnen, so bilden die

$$\Omega(\sqrt{p_k}) \qquad (k=1,\ldots,p-1) \tag{17}$$

eine Basis von $\mathfrak{M}_1$. Hieraus folgt nach [8] (17)

$$e_1 = t-1. \tag{18}$$

Um die Gruppe $\mathfrak{A}_1$ und ein System erzeugender Elemente von ihr anzugeben, nehme man zu jedem System $\mathfrak{S} = (d', d'', m', m'')$ zwei ganze rationale Zahlen x', x'' mit den Bedingungen

$$(x', m'') = 1, \quad (x'', m') = 1, \tag{19}$$

$$d' m'^2 x'^2 - d'' m''^2 x''^2 > 0, \equiv 1 \pmod 2), \tag{20}$$

und setze

$$\xi = m'x'\sqrt{d'} + m''x''\sqrt{d''}. \tag{21}$$

Man nenne ξ kurz eine zu $\mathfrak{S}$ gehörige Zahl. Diese Zahl ξ ist ganz und das Ideal[17] (ξ) *liegt in einer Idealklasse A, die durch $\mathfrak{S}$ eindeutig bestimmt ist, also mit $A(\mathfrak{S})$ bezeichnet werden darf, ferner gilt der Homomorphismus*

$$\mathfrak{G} \sim \mathfrak{A}_1 \quad (\mathfrak{S} \to A(\mathfrak{S})), \tag{22}$$

der wegen $O(\mathfrak{A}_1) = 2^{e_1} = 2^{t-1}$ ein $2:1$ Homomorphismus ist.[18] *Nimmt man also*

[16] Sonst auch werden wir im Falle einer algebraischen Zahl α oder eines Ideals $\mathfrak{a}$ mit $\alpha', \mathfrak{a}'$ stets ein (in jedem Falle näher zu nennendes) Relativkonjugiertes von α bzw. $\mathfrak{a}$ bezeichnen. Wenn wir aber rationale Zahlen mit a', x', D_0' usw. bezeichnen (wie wir das auch bisher schon oft getan haben), so wird hierdurch kein Bezug auf den Konjugiertenbegriff genommen.

[17] Wir meinen das aus den durch ξ teilbaren Elementen von $[\Omega]$ bestehende Ideal.

[18] Nach (22) handelt es sich mit der in [8] § 2 eingeführten Redeweise um eine abundante Erzeugung von $\mathfrak{A}_1$.

eine Basis $\mathfrak{S}^{(1)}, \ldots, \mathfrak{S}^{(t)}$ *von* $\mathfrak{S}$, *so bilden die Klassen*

$$A(\mathfrak{S}^{(i)}) \qquad (i=1,\ldots,t) \tag{23}$$

ein System erzeugender Elemente von $\mathfrak{A}_1$. (Mit der Basis (17) und dem Erzeugendensystem (23) läßt sich der Hauptsatz in [8] § 2 anwenden, so daß man zuerst die Matrix M_1 in (11) aufstellt und dann die Ableitungsfolge $M_1, M_2, \ldots$ in (12) bildet. Da dann e_n mit der Anzahl der Spalten von M_n übereinstimmt, so liefert Satz 1 mit dem Hauptsatz in [8] § 2 zusammen in der Tat die Lösung von Problem I.)

Die erste Hälfte von Satz 1 beweisen wir erst in § 5 (s. den Schluß von Satz 5). Für das übrige beweisen wir zunächst zwei Hilfssätze.

HILFSSATZ 1. *Für jede zu 2 prime Zahl* α *in* $[\Omega]$ *aber außerhalb von* $[\Omega]^{(q)}$ *liegt* α^k $(k=1,2,\ldots)$ *dann und nur dann in* $[\Omega]^{(q)}$, *wenn* $3|k$ *ist.* (Offenbar gilt dann dasselbe für $[\Omega]_m, [\Omega]_m^{(q)}$ statt $[\Omega], [\Omega]^{(q)}$.)[19]

Nach der Annahme muß nämlich

$$\alpha=\frac{x+y\sqrt{d}}{2} \qquad (2\nmid x,y;\, d\equiv 5 \pmod 8)$$

gelten. Hieraus folgt

$$\alpha^3 = x\frac{x^2+3dy^2}{8}+y\frac{3x^2+dy^2}{8}\sqrt{d}.$$

Da hier beide Zähler durch 8 teilbar sind, so gilt $\alpha^3\in[\Omega]^{(q)}$ und allgemeiner $\alpha^k\in[\Omega]^{(q)}$ $(k=3,6,9,\ldots)$. Ferner liegt

$$\alpha^2=\frac{x^2+dy^2}{4}+\frac{xy}{2}\sqrt{d}$$

außerhalb von $[\Omega]^{(q)}$. Wegen $\alpha^3\in[\Omega]^{(q)}$, $(2,\alpha)=1$ gilt auch $\alpha^3\equiv 1 \pmod 2$, woraus

$$\alpha^{3k+1}\equiv\alpha,\quad \alpha^{3k+2}\equiv\alpha^2 \pmod 2 \qquad (k=1,2,\ldots)$$

folgt. Hiernach liegen mit α, α^2 zusammen auch alle $\alpha^{3k+1}, \alpha^{3k+2}$ $(k=1,2,\ldots)$ außerhalb von $[\Omega]^{(q)}$. Somit haben wir Hilfssatz 1 bewiesen.

HILFSSATZ 2. *Die Zahlen* ξ *in* (21) *stimmen mit den Quadratwurzeln aus den zu* $2m$ *primen totalpositiven singulären*[20] *Zahlen von* $[\Omega]_m^{(q)}$ *überein.*

[19] Wenn $x^2-dm^2y^2=-4$ gilt $(2\nmid x,y)$, so liefert die Anwendung von Hilfssatz 1 mit $\alpha=\frac{1}{2}(x+my\sqrt{d})$, daß auch die Gleichung $x^2-dm^2y^2=-1$ lösbar ist. Hiernach würde in Problem IV keine wesentliche Änderung eintreten, wenn man auf der rechten Seite von (4) nicht nur -1, sondern auch -4 stehen läßt. — Hier bemerken wir, daß sich $[\Omega]^{(q)}$ auch als der Unterring derjenigen Elemente von $[\Omega]$ charakterisieren läßt, deren Spur durch 2 teilbar ist. Der wesentliche Inhalt von Hilfssatz 1 läßt sich dann so aussprechen, daß die Spur der zu 2 primen Kubikzahlen in $[\Omega]$ durch 2 teilbar ist. Dementsprechend ließe sich Hilfssatz 1 mit wenigerer Rechnung beweisen, als das oben geschehen wird, er ließe sich natürlich auch leicht verallgemeinern.

[20] Eine Zahl in Ω nennen wir nach HECKE *singulär*, wenn sie das Quadrat eines Ideals in Ω ist.

Nimmt man zu zwei Systemen $\mathfrak{F}, \mathfrak{I}$ $(\in \mathfrak{S})$ je eine zugehörige Zahl ξ, η, so ist auch das Produkt $\xi\eta$ eine der Zahlen (21), *und dieses Produkt gehört dem System $\mathfrak{F}\mathfrak{I}$ zu.*

Zum Beweis dieses Hilfssatzes betrachten wir eine Zahl ξ aus (21). Man betrachte auch das Relativkonjugierte

$$\xi' = m'x'\sqrt{d'} - m''x''\sqrt{d''}.$$

Da die Relativspur $\xi + \xi' = 2m'x'\sqrt{d'}$ ganz ist und die Relativnorm $\xi\xi'$ mit der linken Seite von (20) übereinstimmt, also ebenfalls ganz ist, so folgt das ähnliche auch für ξ. Wegen (19), (20) ist ξ zu $2m$ prim, ferner liegt

$$\varrho = \xi^2 = d'm'^2x'^2 + d''m''^2x''^2 + 2mx'x''\sqrt{d'd''}$$

in $[\Omega]_{m}^{(q)}$. Da d' positiv und singulär[21] ist, so ist wegen

$$d'\xi^2 = (d'm'x' + m''x''\sqrt{d'd''})^2$$

die Zahl ϱ totalpositiv und singulär.

Umgekehrt gehen wir von einer zu $2m$ primen totalpositiven singulären Zahl

(24) $$\varrho = a + b\sqrt{d} \qquad (a, b \text{ ganz rational}; \ m|b)$$

in $[\Omega]_{m}^{(q)}$ aus. Dann ist die Norm von ϱ (positiv sogar) eine ungerade Quadratzahl:

(25) $$a^2 - db^2 = c^2 \qquad (c > 0, \ 2 \nmid a).$$

Diese Gleichung läßt die identische (auf DIRICHLET zurückgehende) Umformung

(26) $$2(a+c)(a+b\sqrt{d}) = (a+c+b\sqrt{d})^2$$

zu. Aus (24), (25), (26) folgt, daß $2(a+c)$ positiv und singulär ist, folglich gilt

(27) $$2(a+c) = rs^2 \qquad (r|D)$$

mit geeigneten natürlichen Zahlen r, s, von denen r quadratfrei angenommen werden darf. Wir zeigen, daß unter den Paaren d', d'' stets ein (übrigens nur ein) solches vorhanden ist, wofür $r = d'$ oder $r = 4d'$, außerdem mit einer natürlichen Zahl u

(28) $$a + c = 2d'u^2$$

gilt. Ist nämlich $r \nmid d$, so ist wegen $r|D$ gewiß $2|r$, $d \equiv 3 \pmod 4$, weshalb man jetzt $d' = \frac{r}{2}\left(d'' = \frac{1}{4}dd'^{-1}\right)$ setzen kann, somit gilt dann (28). Ist $r|d$ und zunächst $2|s$, so kann man $d' = r$ $(d'' = dd'^{-1})$, $u = \frac{s}{2}$ setzen, und dann gilt (28) wieder. Wäre endlich $r|d$, $2 \nmid s$; so folgt aus (27) $2|r$, also $2|d$,

[21] Alle Primfaktoren von D sind nämlich singulär.

woraus sich nach (25) $2a + c$ ergibt, ein Widerspruch mit (27). Wir haben (28) bewiesen.

Nunmehr folgt aus (24), (26), (28)

$$\varrho = (2u\sqrt{d'})^{-2}(2d'u^2 + b\sqrt{d})^2,$$

also

$$\varrho = (u\sqrt{d'} + v\sqrt{d''})^2 \tag{29}$$

mit einer passenden rationalen Zahl v. Da aber ϱ, u ganz sind, so muß wegen (29) auch v ganz sein. Aus (24), (29) folgt

$$m|uv.$$

Da ferner ϱ zu m prim ist, so folgt aus (29) offenbar $(m, uv) = 1$. Also läßt sich mit einem geeigneten Paar m', m''

$$u = m'x', \quad v = m''x'' \tag{30}$$

setzen, so daß für die ganzen Zahlen x', x'' die Bedingungen (19) erfüllt sind. Außerdem folgt aus (24), (29)

$$a = d'u^2 + d''v^2.$$

Dies und (28) ergeben

$$c = d'u^2 - d''v^2.$$

Wegen $c > 0$, $2 \nmid c$ folgt hieraus nach (30) das Bestehen von (20). Wird also

$$\xi = u\sqrt{d'} + v\sqrt{d''}$$

gesetzt, so ist ξ nach (30) eine der Zahlen (21), ferner gilt nach (29) $\sqrt{\varrho} = \xi$. Die erste Hälfte von Hilfssatz 2 haben wir bewiesen.

Dem Beweis der zweiten Hälfte von Hilfssatz 2 schicken wir die Bemerkung voran, daß durch ξ in (21) auch schon das System $\mathfrak{S} = (d', d'', m', m'')$ rückwärts eindeutig bestimmt ist, dem diese Zahl ξ zugehört. Vor allem ist nämlich die Reihenfolge der Glieder auf der rechten Seite von (21) wegen (20_1) eindeutig bestimmt. Folglich ist das im ersten Glied figurierende Radikal $\sqrt{d'}$, also auch d' eindeutig bestimmt. Endlich ist wegen (19_1) auch m' eindeutig bestimmt als der größte gemeinsame Teiler $(m, m'x')$. Somit ist $\mathfrak{S}$, wie behauptet, durch ξ eindeutig bestimmt.

Da die zu $2m$ primen totalpositiven singulären Zahlen von $[\Omega]_m^{(g)}$ offenbar eine Halbgruppe[22] bilden, so gilt ähnliches wegen der schon bewiesenen ersten Hälfte von Hilfssatz 2 auch für die Zahlen in (21). Folglich ist $\xi\eta$ eine der Zahlen (21). Wir haben zu zeigen, daß $\xi\eta$ dem System $\mathfrak{S}\mathfrak{T}$ zugehört. Zu diesem Zweck werde

$$\mathfrak{S} = (d_1', d_1'', m_1', m_1''), \quad \mathfrak{T} = (d_2', d_2'', m_2', m_2''),$$
$$\mathfrak{S}\mathfrak{T} = (d', d'', m', m''),$$
$$\xi = m_1'x'\sqrt{d_1'} + m_1''x''\sqrt{d_1''}, \quad \eta = m_2'y'\sqrt{d_2'} + m_2''y''\sqrt{d_2''}$$

[22] Unter einer Halbgruppe verstehen wir eine multiplikative assoziative (algebraische) Struktur.

gesetzt. Da

$$\xi\sqrt{d_1'}, \quad \eta\sqrt{d_2'}$$

in Ω gehören, so gehört auch ihr Produkt in Ω. Da ferner

$$\sqrt{d_1'}\sqrt{d_2'}\sqrt{d'}$$

rational ist, so folgt, daß $\xi\eta\sqrt{d'}$ in Ω liegt. Deshalb gilt

$$\xi\eta = u\sqrt{d'} + v\sqrt{d''} \tag{31}$$

mit zwei ganzen rationalen Zahlen u, v. Bezeichnen ξ', η' das Relativkonjugierte von ξ, η bezüglich $\mathrm{P}(\sqrt{d_1'})$ bzw. $\mathrm{P}(\sqrt{d_2'})$, so gilt wegen (20_1) $\xi\xi' > 0$, $\eta\eta' > 0$. Für das Relativkonjugierte

$$(\xi\eta)' = u\sqrt{d'} - v\sqrt{d''}$$

von $\xi\eta$ gilt offenbar $(\xi\eta)' = \xi'\eta'$, somit gilt

$$d'u^2 - d''v^2 > 0. \tag{32}$$

Ferner bekommt man

$$u\sqrt{d'} = m_1'm_2'x'y'\sqrt{d_1'd_2'} + m_1''m_2''x''y''\sqrt{d_1''d_2''}. \tag{33}$$

Da

$$d_1'd_2' = 4^k d'a^2, \quad d_1''d_2'' = 4^l d'b^2 \qquad (k, l = 0, -1),$$
$$m_1'm_2' = m'r^2, \qquad m_1''m_2'' = m's^2$$

gelten, wobei a, b, r, s irgendwelche ganze rationale Zahlen sind, so folgt aus (33) $m'|u$. Ähnlich zeigt man $m''|v$. Hieraus und aus (31), (32) folgt nach obiger Bemerkung, daß $\xi\eta$ zum System $\mathfrak{S}\mathfrak{F}$ gehört. Somit haben wir Hilfssatz 2 bewiesen.

Nunmehr können wir die zweite Hälfte von Satz 1 beweisen. Nach Hilfssatz 2 ist ξ ganz und das Ideal $(\xi)^2$ liegt in H_m, also noch mehr in H. Hieraus folgt, daß (ξ) in einer Klasse A liegt. Um zu zeigen, daß A nur von $\mathfrak{S}$ abhängt, betrachten wir neben ξ eine weitere, ebenfalls zu $\mathfrak{S}$ gehörige Zahl

$$\eta = m'y'\sqrt{d'} + m''y''\sqrt{d''},$$

so daß (19), (20) auch für y', y'' statt x', x'' gelten. Es genügt zu zeigen, daß $\xi\eta$ oder $-\xi\eta$ eine totalpositive Ringzahl mod m ist, denn hieraus folgt wegen $(\xi)^2 \in H$, daß $(\xi), (\eta)$ in eine Klasse gehören. Wir berechnen

$$\xi\eta = m'^2x'y'd' + m''^2x''y''d'' + m(x'y'' + x''y')\sqrt{d'd''}.$$

Dies zeigt im Fall $d'd'' = d$ sofort, daß $\xi\eta$ eine Ringzahl mod m ist. Das gleiche gilt auch im Fall $d'd'' = \frac{1}{4}d$, da dann nach (20) x', x'', ebenso auch y', y'' ungerade sein müssen. Wegen (20_1) ist ξ oder $-\xi$ totalpositiv. Das gleiche gilt für η oder $-\eta$, also auch für $\xi\eta$ oder $-\xi\eta$. Die Behauptung haben wir bewiesen, weshalb wir die durch (ξ) repräsentierte Klasse mit $A(\mathfrak{S})$ bezeichnen dürfen.

Aus der zweiten Hälfte von Hilfssatz 2 folgt sofort die Homomorphieeigenschaft

$$A(\mathfrak{s}\mathfrak{t}) = A(\mathfrak{s})A(\mathfrak{t}).$$

Zur Beendigung des Beweises von Satz 1 haben wir nur noch zu zeigen, daß jede Klasse A unter den $A(\mathfrak{s})$ vorkommt. Hierzu nehmen wir ein zu 2 primes ganzes Ideal $\mathfrak{a}$ aus A. Dann gilt $\mathfrak{a}^2 \in H$. Indem man also $\mathfrak{a}$ durch eine ungerade Potenz von ihm ersetzt, läßt sich sogar $\mathfrak{a}^2 \in H_m^+$ annehmen. Hiernach gilt

$$\mathfrak{a}^2 = (\alpha)$$

mit einer zu 2 primen totalpositiven Zahl α in $[\Omega]_m$. Ersetzt man noch $\mathfrak{a}$ nötigenfalls durch $\mathfrak{a}^3$, so wird nach Hilfssatz 1 sogar $\alpha \in [\Omega]_m^{(n)}$ gelten. Aus Hilfssatz 2 folgt dann, daß $\alpha = \xi^2$ gilt mit einer Zahl ξ aus (21). Hierfür gilt $(\xi) = \mathfrak{a}$. Da hiernach (ξ) in A liegt, so bedeutet dies, daß A unter den Klassen $A(\mathfrak{s})$ vorkommt. Somit haben wir die zweite Hälfte von Satz 1 bewiesen.

§ 4. Lösung der Probleme II bis IV

Satz 2. *Die Systeme $\mathfrak{s} = (d', d'', m', m'')$, für die die Diophantische Gleichung* (2) *lösbar ist, bilden (bei festen d, m, n) eine Untergruppe $\mathfrak{S}_n$ von $\mathfrak{S}$ mit*

(34) $$O(\mathfrak{S}_n) = 2^{1+r_{n+1}},$$

(35) $$\mathfrak{S}_1 \supseteq \cdots \supseteq \mathfrak{S}_{r-1} \supset \mathfrak{S}_r = \mathfrak{S}_{r+1} = \cdots \qquad (O(\mathfrak{S}_r) = 2).$$

Um $\mathfrak{S}_n (n = 1, 2, \ldots)$ zu bestimmen, reduziere man die am Ende von Satz 1 genannte Matrix M_n aus,[23] *fasse dann die in den aus lauter Elementen 1 bestehenden Zeilen vorkommenden Nenner $A(\mathfrak{s})$ ins Auge; die in diesen figurierenden $\mathfrak{s}$ bilden eine Basis von $\mathfrak{S}_n$.*

Zusatz. *Die Elemente von $\mathfrak{S}_n$ $(n = 1, \ldots, r)$ lassen sich auch so charakterisieren: Das System $\mathfrak{s}$ gehört dann und nur dann zu $\mathfrak{S}_n$, wenn*

(36) $$\left(\frac{K}{A(\mathfrak{s})}\right)_n = 1$$

für alle diejenigen K gilt, für die die linke Seite existiert.[24]

Bemerkung. Nach dem Zusatz in [8] § 2 gilt

(37) $$A(\mathfrak{s}) = H \qquad (\mathfrak{s} \in \mathfrak{S}_r).$$

Genauer bedeutet das wegen $O(\mathfrak{S}_r) = 2$, daß $\mathfrak{S}_r$ eben der Kern der Homomorphie (22) ist.

23 Es genügt auch, daß man M_n nach den Zeilen reduziert, d. h. den e_{n+1}-Schritt unseres Algorithmus ausführt (vgl. [8] § 3).

24 Diese K machen nach [8] Satz 5 eben die Menge $\mathfrak{M}_n$ aus.

Satz 3. *Es gibt (bei festen d, m) genau zwei Systeme* $\mathfrak{s}=(d', d'', m', m'')$, *für die die Dirichletsche Gleichung* (3) *lösbar ist. Diese* $\mathfrak{s}$ *machen eben die im Satz* 2 *genannte Gruppe* $\mathfrak{S}_\nu$ *aus.*

Bemerkung. Man setze einen Augenblick $\mathfrak{S}=\mathfrak{S}_n$ und zerlege $\mathfrak{S}_n$ in ein direktes Produkt

$$\mathfrak{S}_n=\mathfrak{S}_\nu \times \mathfrak{S}_n' \qquad (n= 0, \ldots, \nu-1).$$

Aus voriger Bemerkung folgt wegen (22), daß die

$$A(\mathfrak{s}) \qquad (\mathfrak{s}\in\mathfrak{S}_n')$$

die sämtlichen verschiedenen Elemente der Gruppe $\mathfrak{A}_{n+1}$ sind $(n=0, \ldots, \nu-1)$. Läßt man $\mathfrak{s}$ eine Basis von $\mathfrak{S}_n'$ durchlaufen, so durchläuft $A(\mathfrak{s})$ eine Basis von $\mathfrak{A}_{n+1}$. Hiernach ist die schon im § 1 erwähnte körpertheoretische Bedeutung der Probleme II, III klar.

Satz 4. *Die Pellsche Gleichung* (4) *ist dann und nur dann lösbar, wenn* ($d>0$ *und*) *das vom Einselement* $\mathfrak{s}_1=(1, d, 1, m)$ *verschiedene Element der in den Sätzen* 2, 3 *genannten Gruppe* $\mathfrak{S}_\nu$ *gleich* ($\mathfrak{s}_1^* =$) $(d, 1, m, 1)$ *ist.*

Zum Beweis brauchen wir drei Hilfssätze.

Hilfssatz 3. *Die Gruppe der totalpositiven Einheiten in* $[\Omega]_{m}^{(q)}$ *ist zyklisch und ihre Ordnung ist im Fall* $d>0$ *unendlich, im Fall* $d<0$ *eine gerade Zahl.*

Im Fall $d>0$ handelt es sich nämlich um die Einheiten

$$(x+my\sqrt{d})^k \qquad (k=0, \pm 1, \ldots),$$

wobei x, y die kleinste positive Lösung der Pellschen Gleichung

$$x^2-dm^2y^2=1$$

ist. Im Fall $d<0$ sind die genannten Einheiten $\pm 1, \pm\sqrt{-1}$ bzw. ± 1, je nachdem $dm^2=-1$ oder <-1 ist. Hiernach ist Hilfssatz 3 in allen Fällen richtig.

Hilfssatz 4. *Ist* ε *ein erzeugendes Element der (zyklischen) Gruppe der totalpositiven Einheiten in* $[\Omega]_{m}^{(q)}$, *so ist* $\sqrt{\varepsilon}$ *eine der Zahlen in* (21). *Bezeichne* $\mathfrak{s}_\infty(\in\mathfrak{S})$ *das System, dem* $\sqrt{\varepsilon}$ *zugehört, und zwar setze man*

$$\mathfrak{s}_\infty=(d_\infty', d_\infty'', m_\infty', m_\infty''),$$

$$\sqrt{\varepsilon}=m_\infty' x_\infty' \sqrt{d_\infty'}+m_\infty'' x_\infty'' \sqrt{d_\infty''} \qquad (x_\infty', x_\infty''\in[\mathrm{P}]).$$

Das System $\mathfrak{s}_\infty$ *ist vom Einselement* $\mathfrak{s}_1=(1, d, 1, m)$ *verschieden, und es gilt*

$$d_\infty' m_\infty'^2 x_\infty'^2-d_\infty'' m_\infty''^2 x_\infty''^2=1, \tag{38}$$

weshalb $\sqrt{\varepsilon}$ *eine Lösung der dem System* $\mathfrak{s}_\infty$ *zugehörenden Gleichung* (3) *liefert. Außerdem gilt*

$$A(\mathfrak{s}_\infty)=H. \tag{39}$$

Bemerkung. Dieser Hilfssatz mit Satz 3 zusammen besagt, daß $\mathfrak{S}_1$ und $\mathfrak{S}_\alpha$ eben die Gruppe $\mathfrak{S}_r$ ausmachen (was wir im § 1 vorweggenommen und dort $\mathfrak{S}_\alpha$ durch *diese* Eigenschaft definiert haben).

Um Hilfssatz 4 zu beweisen, berücksichtige man, daß jede Einheit in $[\Omega]$ eine singuläre Zahl ist. Hieraus folgt nach Hilfssatz 2, daß $\sqrt{\varepsilon}$ in der Tat eine der Zahlen (21) ist. Da $\sqrt{\varepsilon}$ eine Einheit ist, so liegt das Ideal $(\sqrt{\varepsilon})$ in der Hauptklasse H, woraus (39) folgt. Man braucht nur noch $\mathfrak{S}_\alpha \neq \mathfrak{S}_1$ zu beweisen, denn die übrigen Behauptungen von Hilfssatz 4 sind klar. Wäre $\mathfrak{S}_\alpha = \mathfrak{S}_1$, so würde (38) besagen, daß $\sqrt{\varepsilon}$ oder $-\sqrt{\varepsilon}$ ein Element der im Hilfssatz 4 genannten Gruppe ist. Das ist aber wegen Hilfssatz 3 unmöglich. Mit diesem Widerspruch haben wir Hilfssatz 4 bewiesen.

Hilfssatz 5 *Die Gleichung* (2) *ist dann und nur dann lösbar, wenn für* $\mathfrak{S} = (d', d'', m', m'')$ *die Klasse* $A(\mathfrak{S})$ *eine* 2^n*-te Potenz ist* (d. h. in $\mathfrak{A}_{n+1}$ liegt).

Nehmen wir nämlich zuerst an, daß es zu $\mathfrak{S}$ eine Lösung x', x'', z von (2) gibt. Dann sind die Bedingungen (19), (20) offenbar erfüllt. Wir betrachten die entsprechende Zahl ξ in (21) und auch ihre Relativkonjugierte

$$\xi' = m'x'\sqrt{d'} - m''x''\sqrt{d''}.$$

Die Ideale (ξ), (ξ') sind wegen (2) zueinander prim, ferner gilt $\xi\xi' = z^{2^n}$. Hiernach ist (ξ) eine 2^n-te Idealpotenz in Ω. Nach Satz 1 folgt hieraus, daß $A(\mathfrak{S})$ eine 2^n-te Potenz ist.

Umgekehrt sei

$$A(\mathfrak{S}) = C^{2^n} \tag{40}$$

mit einer Klasse C. Wir nehmen ein ganzes, zu $2dm$ primes, durch keine rationale Primzahl teilbares Ideal $\mathfrak{c}$ aus C und setzen

$$\mathfrak{a} = \mathfrak{c}^{2^n}. \tag{41}$$

Dann liegt $\mathfrak{a}^2$ in H. Indem wir $\mathfrak{c}$ durch eine passende ungerade Potenz von ihm ersetzen, können wir erreichen, daß $\mathfrak{a}^2$ in $H_{\tilde{m}}$ liegt. Dann gilt

$$\mathfrak{a}^2 = (\alpha) \tag{42}$$

mit einer zu $2dm$ primen totalpositiven Ringzahl α mod m. Ersetzt man $\mathfrak{c}$ nötigenfalls durch $\mathfrak{c}^8$, so erreicht man nach Hilfssatz 1, daß α sogar in $[\Omega]_m^{(g)}$ liegt. Da α nach (42) auch singulär ist, so folgt aus Hilfssatz 2

$$\alpha = \xi^2 \tag{43}$$

mit einer Zahl ξ in (21), die aber jetzt nicht notwendig zum System $\mathfrak{S}$ gehört. Wir bezeichnen mit $\mathfrak{T}(\in\mathfrak{S})$ das System, dem ξ zugehört, und zeigen, daß nach passender Wahl von α trotzdem $\mathfrak{T} = \mathfrak{S}$ ausfällt. Nach Satz 1 liegt das Ideal (ξ) in $A(\mathfrak{T})$. Andererseits ist nach (42), (43) $\mathfrak{a} \doteq (\xi)$, somit folgt aus (41)

$$A(\mathfrak{T}) = A(\mathfrak{S}). \tag{44}$$

Hieraus folgt $\mathfrak{T} = \mathfrak{S}$ natürlich nicht, aber jetzt wollen wir berücksichtigen, daß man in (42) für α auch $\alpha\varepsilon$ nehmen darf, wobei α dieselbe Einheit ist wie im Hilfssatz 4. An Stelle von (43) haben wir dann die entsprechende Gleichung

$$\alpha\varepsilon = (\xi\sqrt{\varepsilon})^2.$$

Nach den Hilfssätzen 2, 4 gehört die Zahl $\xi\sqrt{\varepsilon}$ dem System $\mathfrak{T}\mathfrak{S}_\infty$ zu, weshalb mit (44) zusammen auch die ähnliche Gleichung

$$A(\mathfrak{T}\mathfrak{S}_\alpha) = A(\mathfrak{S}) \tag{45}$$

gelten muß. Da $\mathfrak{S}_\infty \neq \mathfrak{S}_1$ ist, so ist $\mathfrak{T}\mathfrak{S}_\infty \neq \mathfrak{T}$. Da ferner (22) eine $2:1$ Homomorphie ist, so folgt aus (44), (45), daß $\mathfrak{T}$ oder $\mathfrak{T}\mathfrak{S}_\infty$ mit $\mathfrak{S}$ übereinstimmt. Hiernach können wir durch die passende Wahl von α in der Tat erreichen, daß selbst schon ξ dem System $\mathfrak{S}$ zugehört.

Dann gilt

$$\xi = m'x'\sqrt{d'} + m''x''\sqrt{d''} \tag{46}$$

so, daß dabei (19), (20) befriedigt sind. Da ferner nach (42), (43) $\mathfrak{a} = (\xi)$ ist, so folgt aus (41)

$$(\xi) = \mathfrak{c}^{2^n}. \tag{47}$$

Dabei ist mit $\mathfrak{a}$ zusammen auch $\mathfrak{c}$ und die Norm von $\mathfrak{c}$ zu $2dm$ prim. Wird diese Norm mit z bezeichnet, so ergibt sich wegen (20_1), (46), (47)

$$d'm'^2x'^2 - d''m''^2x''^2 = z^{2^n}.$$

Ferner hat mit $\mathfrak{c}$ zusammen auch $\mathfrak{a} = (\xi)$ keinen rationalen Primzahlteiler, weshalb wegen $(z, 2dm) = 1$

$$(m'x', m''x'', z) = 1, \; 2 \nmid z$$

ist. Wir haben bekommen, daß (2) lösbar ist, womit wir Hilfssatz 5 bewiesen haben.

Nunmehr beweisen wir Satz 2. Nach [8] (17) ist

$$O(\mathfrak{A}_{n+1}) = 2^{e_{n+1}},$$

ferner gilt $\mathfrak{A}_1 \supseteq \mathfrak{A}_2 \supseteq \cdots$. Hiernach folgt aus Hilfssatz 4 und der $2:1$ Homomorphie (22) die Richtigkeit von (34), (35), wobei man auch (1) zu berücksichtigen hatte. Die Anzahl der im Satz 2 genannten Nenner $A(\mathfrak{S})$ ist $1 + e_{n+1}$, sie bilden ferner ein System erzeugender Elemente von $\mathfrak{A}_{n+1}$, endlich sind die in ihnen figurierenden $\mathfrak{S}$ unabhängige Elemente von $\mathfrak{S}$. Hieraus und aus der Homomorphie (22) folgt wegen Hilfssatz 4 die restliche Behauptung von Satz 2.

Nach dem Schluß von [8] Lemma 3 und nach [8] Satz 5 besteht $\mathfrak{A}_{n+1} (n = 1, \ldots, \nu)$ aus denjenigen A, für die

$$\left(\frac{K}{A}\right)_n = 1$$

gilt, immer wenn die linke Seite existiert. Hiernach folgt aus Hilfssatz 4 die Richtigkeit des Zusatzes.

Der Beweis von Satz 3 erfolgt so. Nach dem Anfang von Hilfssatz 4 ist $\varepsilon_0 = \sqrt{\varepsilon}$ eine der Zahlen (21). Für diese Zahl ist die linke Seite von (20) gleich 1, somit haben wir es mit einer lösbaren Gleichung (3) zu tun. Und zwar ist das zugehörige System, wie wir das auch gesehen haben, von $\mathfrak{S} = (1, d, 1, m)$ verschieden. Ferner ist (3) auch noch im Fall $\mathfrak{S} = \mathfrak{S}_1$ lösbar. Andererseits ist klar, daß (3) für kein $\mathfrak{S}$ außerhalb von $\mathfrak{S}_r$ lösbar sein kann. Hiernach folgt aus (35) die Richtigkeit von Satz 3.

Da (4) der zum System $\mathfrak{S}_1^*$ gehörende Spezialfall von (3) ist, so folgt aus Satz 3 die Richtigkeit von Satz 4.

§ 5. Die Eigenschaften der Ringklassenkörper

Wohl haben wir unsere Probleme I bis IV in den Sätzen 1 bis 4 beantwortet, aber wir wissen auch (vgl. [8] §§ 1, 6), daß zur Anwendung auf konkrete Fälle die effektive Konstruktion der Körper K_n nötig ist. Deshalb wollen wir hier die Eigenschaften der Körper K_n in solcher Ausführlichkeit untersuchen, daß wir diese Körper dann im folgenden § 6 konstruieren können.

Zur vorherigen Beleuchtung unseres Verfahrens bemerken wir folgendes. Ganz allgemein, wenn man einen Körper K konstruieren will, so zerlegt man ihn oft zweckmäßig in ein Produkt $K = K_1 \cdots K_r$ von möglichst einfach gebauten Körpern $K_1, \ldots, K_r$. Insbesondere, wenn es sich um algebraische Zahlkörper endlichen Grades handelt (nachher wollen wir in dieser Arbeit stets nur noch von solchen Körpern reden), so kann man verlangen, daß die Faktoren K_i von möglichst kleinem Grade sind. Freilich gibt im betrachteten Falle die Theorie von Galois genaue Auskunft über alle Zerlegungsmöglichkeiten. Es wird sich nun in unserem Falle $K = \mathsf{K}_n$ zeigen, daß jede Zerlegung von K_n in ein Produkt von echten Unterkörpern notwendig einen „unzerlegbaren" Faktor A_n vom Grade 2^n enthält. Es wird sich auch zeigen, daß umgekehrt stets eine Zerlegung von der Form $\mathsf{K}_n = \mathsf{A}_n \Omega_n$ existiert, in der also die Faktoren den Grad 2^n bzw. 2 haben. Deshalb verfahren wir natürlicherweise so, daß wir in diesem § 5 die Eigenschaften von K_n durch die eines solchen Körpers A_n untersuchen und im § 6 die Konstruktion von K_n auf die von A_n zurückführen. Das wird gewiß der beste, und wie wir sehen werden, auch sehr gut gangbare Weg zur Konstruktion der Körper K_n.

Der einzige Gegenstand von diesem § 5 wird nur noch der Beweis vom folgenden sehr langen aber leichten:[25]

[25] Für den Spezialfall $m = 1$ geht obiger Satz im wesentlichen auf Reichardt [22] zurück.

SATZ 5. *Man betrachte ein beliebiges festes* K_n $(n=1,\dots,\nu)$ *und zugleich auch die durch dieses eindeutig bestimmte Körperkette*

$$(\Omega=)K_0\subset K_1\subset\cdots\subset K_n. \tag{48}$$

Dann gelten die folgenden 1° *bis* 7°:

1°. *Der Körper* K_n *ist Galoissch (vom Grade* 2^{n+1}*). Seine Galoissche Gruppe läßt sich in der Form*

$$\mathfrak{G}(K_n)=\{T_n,U_n\} \tag{49}$$

annehmen, wobei

$$T_n^{2^n}=1,\quad U_n^2=1,\quad U_nT_nU_n^{-1}=T_n^{-1}. \tag{50}$$

Hiernach ist (49) *die Diedergruppe von der Ordnung* 2^{n+1} *(im Fall* $n=1$ *die Vierergruppe). Folglich enthält* K_n *zu jedem* i $(=1,\dots,n)$ *außer* K_{i-1} *genau* 2^i *Unterkörper vom Grade* 2^i. *Bezeichne* A_i *einen dieser Körper, ferner werde* $A_0=P$ *gesetzt. Es gilt*

$$K_i=A_i\Omega=A_i(\sqrt{D})\qquad (i=1,\dots,n). \tag{51}$$

Für $i=1,\dots,n$ *enhält jedes* A_i *genau ein* A_{i-1} *und jedes* A_{i-1} *ist in genau zwei* A_i *enthalten. Wir wählen im folgenden ein* A_n *fest*[26] *und definieren* $A_1,\dots,A_{n-1}$ *eindeutig so, daß*

$$(P=)A_0\subset A_1\subset\cdots\subset A_n \tag{52}$$

gilt, ferner soll $\bar{A}_i$ $(i=1,\dots,n)$ *den „zweiten" der gesagten Körper über* A_{i-1} *bezeichnen. Wir veranschaulichen die Sachlage so:*

$$\begin{tikzcd}[column sep=small] & K_1 \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\ \Omega \arrow[dr, dash] & A_1 \arrow[d, dash] & \bar{A}_1 \arrow[dl, dash] \\ & P & \end{tikzcd} \qquad \begin{tikzcd}[column sep=small] & K_i \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\ K_{i-1} \arrow[dr, dash] & A_i \arrow[d, dash] & \bar{A}_i \arrow[dl, dash] \\ & A_{i-1} \arrow[d, dash] & \\ & A_{i-2} & \end{tikzcd} \qquad (i=2,\dots,n). \tag{53}$$

Die Automorphismen T_n, U_n *wählen wir so, daß*

$$\mathfrak{G}(K_n|\Omega)=\{T_n\} \tag{54}$$

gilt und A_n *zur Untergruppe* $\{U_n\}$ *von* (49) *gehört.*[27]

2°. *Die Primidealfaktoren von* D *in* Ω *zerfallen in* $K_{n-1}|\Omega$ *voll.*

[26] Umgekehrt ist durch A_n und Ω auch schon $K_n=A_n\Omega$ eindeutig bestimmt. (Für $n\geqq 2$ ist K_n sogar durch A_n allein bestimmt als sein Galoisscher Körper.) Die oben bis (64) zu definierenden Begriffe A_i, $\bar{A}_i$, $\mathfrak{d}_i$, $\mathfrak{d}'_i$, $\mathfrak{m}_i$, m_i, α_i, α'_i (vgl. aber [32]) werden lauter Invarianten von K_n und A_n (teils nur von K_n) bedeuten. Unser Satz 5 ist im wesentlichen der Inbegriff der Eigenschaften dieser Invarianten.

[27] Zur Wahl von T_n gibt es genau 2^{n-1} Möglichkeiten. Würde man neben A_n noch einen Unterkörper B_n von K_n vom Grade 2^n mit $A_n\cap B_n=P$ auszeichnen und T_n so definieren, daß B_n zur Untergruppe $\{T_nU_n\}$ gehört, so wäre hierdurch auch T_n eindeutig festgelegt. Das wird aber für uns unnötig, ferner werden wir unter allen Unterkörpern von K_n nur die in (53) markierten zu betrachten haben.

3°. *Insbesondere gilt*

(55) $$\mathrm{A}_1 = \mathrm{P}(\sqrt{D_0 m_1}) \qquad (m_1 \mid m)$$

mit einer primären ganzen Zahl m_1 *und einer D-Zerfällung* D_0, D_0', *die im Fall* $m_1 = 1$ *echt ist.*

4°. *Es gilt*[28]

(56) $$D_{\mathrm{A}_{i+1}|\mathrm{A}_i} = \mathfrak{d}_i \mathfrak{m}_i \qquad (\mathfrak{d}_i \mid D, \mathfrak{m}_i \mid m;\ i = 0, \ldots, n-1)$$

mit eindeutig bestimmten (ganzen) Idealen $\mathfrak{d}_i, \mathfrak{m}_i$ *in* A_i. *Die* $\mathfrak{m}_i$ *sind selbstkonjugiert*[29] *und zwar ist*

(57) $$\mathfrak{m}_i = m_{i+1} m_i^{2^{-1}} \cdots m_1^{2^{-i}} \qquad (i = 0, \ldots, n-1)$$

mit eindeutig bestimmten primären ganzen rationalen Zahlen $m_2, \ldots, m_n$, *für die (mit obigem* m_1 *zusammen)*

(58) $$m_1 \cdots m_n \mid m$$

gilt.[30] *Für die* $\mathfrak{d}_i$ *gilt*

(59) $$\mathfrak{d}_0 = D_0,\ \mathfrak{d}_1 \mathfrak{d}_1' = D_0',\ \mathfrak{d}_i \mathfrak{d}_i' = \mathfrak{d}_{i-1}' \qquad (i = 2, \ldots, n-1),$$

wobei $\mathfrak{d}_i'$ $(i = 1, \ldots, n-1)$ *das Konjugierte von* $\mathfrak{d}_i$ *in* $\mathrm{A}_i|\mathrm{A}_{i-1}$ *ist.*[31] *Außerdem gelten*

(60) $$(\mathfrak{d}_i, \mathfrak{d}_i') = 1$$

(61) $$\mathfrak{d}_0 \cdots \mathfrak{d}_i \mathfrak{d}_i' = D \qquad (i = 1, \ldots, n-1).$$

(62) $$N_{\mathrm{A}_i} \mathfrak{d}_i = D_0'$$

5°. *Wir setzen (vgl.* (55₁)*)*

(63) $$\mathrm{A}_{i+1} = \mathrm{A}_i(\sqrt{\alpha_i}) \qquad (\alpha_0 = D_0 m_1;\ i = 0, \ldots, n-1)$$

mit geeigneten Zahlen α_i *in* A_i.[32] *Es gelten (vgl.* (59)*)*[33]

(64) $$\alpha_0 = D_0 m_1,\ \alpha_1 \alpha_1' \underset{(2)}{=} D_0' m_1 \text{ (in P)},\ \alpha_i \alpha_i' \underset{(2)}{=} \alpha_{i-1}' \text{ (in } \mathrm{A}_{i-1}) \qquad (i = 2, \ldots, n-1),$$

[28] $D_{L|K}, N_{L|K}, S_{L|K}$ bezeichnen die Diskriminante eines Relativkörpers $L|K$ und die Norm bzw. Spur in $L|K$. Wenn $K = \mathrm{P}$ ist, so schreiben wir kurz D_L, N_L, S_L.

[29] Selbstkonjugiert nennen wir ein Ideal, wenn es mit allen Konjugierten gleich ist.

[30] Obiges (57) hat den Sinn, daß $m_1^{2^{-1}}, \ldots, m_i^{2^{-i}}$ der Reihe nach Ideale $\mathfrak{a}_1, \ldots, \mathfrak{a}_i$ in A_i bezeichnen, für die $\mathfrak{a}_1^2 = m_1, \ldots, \mathfrak{a}_i^{2^i} = m_i$ gilt.

[31] Nach (59) gelten die Teilbarkeiten $\mathfrak{d}_{n-1}' | \ldots | \mathfrak{d}_1' | D_0'$. Dagegen sind $\mathfrak{d}_0, \ldots, \mathfrak{d}_{n-1}$ wegen (59), (60) paarweise relativ prim. Man bemerke auch die Folgerung von (59), (60), daß in $\mathrm{A}_i|\mathrm{A}_{i-1}$ $(i = 1, \ldots, n-1)$ alle Primidealfaktoren von $\mathfrak{d}_{i-1}'$ voll zerfallen. Das bedeutet jetzt, daß sie in ein Produkt von zwei verschiedenen Primidealen zerfallen. Im allgemeinen, wenn $L|K$ ein Relativkörper vom Grad r ist und $\mathfrak{p} = \mathfrak{P}_1 \ldots \mathfrak{P}_r$ gilt, wobei $\mathfrak{p}$ und $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ Primideale in K bzw. L bezeichnen, so sagen wir, daß $\mathfrak{p}$ in $L|K$ voll zerfällt bzw. voll verzweigt, je nachdem die $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ verschieden bzw. alle gleich sind.

[32] Offenbar ist α_i bis auf einen willkürlichen, von 0 verschiedenen Quadratzahlfaktor in A_i eindeutig bestimmt. Anders gesagt ist also die „Quadratklasse" von α_i (in A_i) eine Invariante (von $\mathrm{K}_n, \mathrm{A}_n$). Deshalb dürfen die α_i als ganze Zahlen gewählt werden. Man bemerke, daß wegen (52), (63) die Zahl $\sqrt{\alpha_i}$ vom Grad 2^{i+1} also α_i vom Grad 2^i sein muß.

wobei α'_i das Konjugierte von α_i in $\mathsf{A}_i|\mathsf{A}_{i-1}$ bezeichnet. Ferner gelten

$$\left.\begin{array}{lll}(65) & (\alpha_i) \underset{(2)}{=} \mathfrak{d}_i\mathfrak{m}_i & \\ (66) & \alpha_i \underset{(2)}{\equiv} 1 \left(\mathrm{mod}\ \dfrac{4}{(2,\mathfrak{d}_i)^2}\right) & \Big\} \text{ (in } \mathsf{A}_i) \\ (67) & \alpha_i \cdot T_n \alpha_i \underset{(2)}{=} 1 \quad (\text{in } \mathsf{K}_i) & \end{array}\right\} \quad (i=0,\ldots,n-1).$$

Es bestehen noch (vgl. (55))

$$\left.\begin{array}{ll}(68) & \bar{\mathsf{A}}_1 = \mathsf{P}(\sqrt{D'_0 m_1}),\ \bar{\mathsf{A}}_{i+1} = \mathsf{A}_i(\sqrt{\alpha_i}) \\ (69) & \mathsf{K}_1 = \Omega(\sqrt{D_0 m_1}) = \Omega(\sqrt{D'_0 m_1}),\ \mathsf{K}_{i+1} = \mathsf{K}_i(\sqrt{\alpha_i}) = \mathsf{K}_i(\sqrt{\alpha'_i}) \end{array}\right\} (i=1,\ldots,n-1).$$

6°. *Es gelten (vgl. (56))*

$$(70) \qquad D_{\bar{\mathsf{A}}_1} = D'_0 m_1, \quad D_{\bar{\mathsf{A}}_{i+1}|\mathsf{A}_i} = \mathfrak{d}'_i\mathfrak{m}_i \qquad (i=1,\ldots,n-1),$$

$$(71) \qquad D_{\mathsf{K}_{i+1}|\mathsf{K}_i} = \mathfrak{m}_i \qquad (i=0,\ldots,n-1).$$

7°. *Über K_{n-1} $(2 \leqq n \leqq \nu)$ gibt est genau 2^{t-2} Körper K'_n, diese werden, jeder genau viermal, durch*

$$(72) \qquad \mathsf{K}^*_n = \mathsf{K}_{n-1}(\sqrt{D^* m^* \alpha_{n-1}}) \qquad (D^*|D,\ m^*|m)$$

angegeben, wobei man diejenigen ganzen rationalen Teiler D^*, m^* von D bzw. m zuzulassen hat, für die D^*, DD^{*-1} eine D-Zerfällung und m^* primär ist.[34] *Und zwar bekommt man aus einem Körper* (72) *die übrigen drei, ihm gleichen so, daß man $D^* m^*$ mit $D, D_0 m_1, D'_0 m_1$ multipliziert und nachher die Primzahlquadratfaktoren streicht (vgl.* (69_1)*). Offenbar ist jetzt*

$$\mathsf{A}^*_n = \mathsf{A}_{n-1}(\sqrt{D^* m^* \alpha_{n-1}})$$

ein von K_n verschiedener Körper (2^n-ten Grades) mit $\mathsf{A}_{n-1} \subset \mathsf{A}^*_n \subset \mathsf{K}^*_n$, den man also im Zusammenhang mit K^*_n an Stelle von A_n nehmen kann. Bezeichnen ferner m^*_n, $\mathfrak{d}^*_{n-1}$ den Wert von m_n, $\mathfrak{d}_{n-1}$ bezüglich K^*_n, A^*_n (statt K_n, A_n), so gilt

$$(73) \qquad m^*_n \underset{(2)}{=} \frac{m^* m_n}{(m^*, m_1 \cdots m_{n-1})} \ (\text{in } \mathsf{P}), \quad \mathfrak{d}^*_{n-1} = (D^*, \mathfrak{d}'_{n-1})(DD^{*-1}, \mathfrak{d}_{n-1}).$$

Bezüglich des übriggebliebenen Falles $n=1$ gilt: Es gibt genau $2^{t-1}-1$ Körper K'_1. Diese werden, jeder genau zweimal, durch

$$(74) \qquad \mathsf{K}^*_1 = \Omega(\sqrt{D^* m^*})$$

angegeben, wobei D^*, m^* dasselbe bedeuten wie in (72) *mit dem Unterschied, daß im Fall $m^* = 1$ die D-Zerfällung D^*, DD^{*-1} echt sein soll. Und zwar bekommt man aus einem Körper* (74) *den anderen, ihm gleichen so, daß man*

[33] Wie üblich bezeichnet „$\underset{(2)}{=}$" und „$\underset{(2)}{\equiv}$" die Gleichheit bzw. Kongruenz bis auf einen von 0 verschiedenen Quadratfaktor, dessen Basis stets sinngemäß eine Zahl oder ein Ideal eines, in jedem Falle anzugebenden Körpers ist.

[34] Insbesondere für $D^* = m^* = 1$ stimmt K^*_n mit obigem K_n überein.

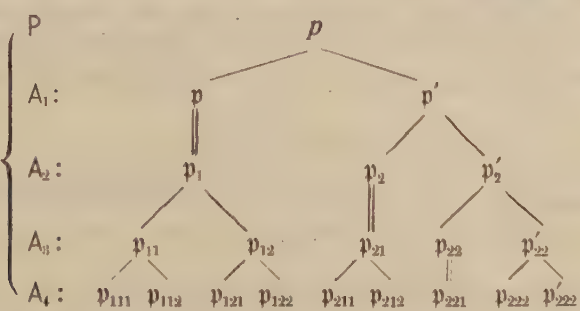
D^* durch $D D^{*-1}$ ersetzt. Für (74) *und den entsprechenden Körper* $A_1^* = P(\sqrt{D^* m^*})$ *fällt* $m_1 = m^*$ *bzw.* $\mathfrak{d}_0 = D^*$ *aus.*[35]

BEMERKUNG. Aus (71), (57) folgt wegen $K_0 = P(\sqrt{D})$, daß unter allen Primzahlen genau nur die Faktoren von $D m_1 \ldots m_n$ in K_n verzweigen. Wir wollen näher zusehen, wie diese Primzahlen p in K_n und ihren Unterkörpern in Primideale zerlegt werden. Zunächst folgt aus 2⁰, daß im Fall $p | D$

$$p = (\mathfrak{p}_1 \ldots \mathfrak{p}_r)^2 \qquad (r = 2^{n-1}) \tag{75}$$

gilt mit verschiedenen Primidealen $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ ersten Grades in K_n. Wegen (55) folgt hieraus: *Erstens* wenn $p | D_0$ ist, so gilt $p = \mathfrak{p}^2$ mit einem Primideal $\mathfrak{p}$ ersten Grades in A_1, ferner zerfällt dieses in $A_{n-1} | A_1$ $(n \geqq 2)$ voll. *Zweitens* wenn $p | D_0'$ ist, so folgt aus vorigem wegen (55), (56), (59) offenbar, daß p der Reihe nach in den Körpern $A_1, \ldots, A_{n-1}$ nach folgendem Schema in Primideale ersten Grades zerfällt (veranschaulicht wird der Fall $n = 5$):

(76)



Die divergenten und parallelen Linienpaare veranschaulichen die Vollzerfällung bzw. die Vollverzweigung. Die letzten zwei Primideale in der mit A_i markierten Zeile sind eben $(p, \mathfrak{d}_i)$ bzw. $(p, \mathfrak{d}_i')$. Diese zwei gehen in p zur ersten Potenz, die übrigen $2^{i-1} - 1$ Primideale der gesagten Zeile zur zweiten Potenz auf. *Drittens* wenn $p | m_i$ $(1 \leqq i \leqq n)$ ist, so folgt aus (56), (57), daß p in $A_0, \ldots, A_i$ unverzweigt ist und die Primidealfaktoren von p in A_i in den Körpern $A_{i+1}, \ldots, A_n$ vollverzweigen; dasselbe gilt wegen (71) auch für „K" statt „A".

[35] Man sieht, daß der Teil 7⁰ von anderer Natur ist, als die vorigen Teile 1⁰ bis 6⁰ des Satzes, da es sich in diesen um die Eigenschaften eines festen K_n und eines in ihm enthaltenen A_n handelt, während 7⁰ besagt, wie alle Paare K_n, A_n über einem festen Paar K_{n-1}, A_{n-1} beschaffen sind $(1 \leqq n \leqq \nu)$. — Wir bemerken, daß die rechte Seite von (73_2) für die verschiedenen D^* alle überhaupt möglichen ganzen Ideale $\mathfrak{d}_{n-1}^*$ mit den Eigenschaften

$$\mathfrak{d}_{n-1}^* \mathfrak{d}_{n-1}^{*\prime} = \mathfrak{d}_{n-2}', \quad (\mathfrak{d}_{n-1}^*, \mathfrak{d}_{n-1}^{*\prime}) = 1$$

durchläuft, wobei $\mathfrak{d}_{n-1}^{*\prime}$ das Konjugierte von $\mathfrak{d}_{n-1}^*$ in $A_{n-1} | A_{n-2}$ bezeichnet. Das folgt nämlich leicht daraus, daß nach (59_3), (60) insbesondere auch $\mathfrak{d}_{n-1}$ eins der hier gesagten Ideale $\mathfrak{d}_{n-1}^*$ ist. Man sieht sogar, daß (73_2) auch schon dann die sämtlichen verschiedenen $\mathfrak{d}_{n-1}^*$ liefert, wenn man für D^* nur die Teiler von D_0' zuläßt. Dies folgt daraus, daß nach $(59_{2,3})$ alle $\mathfrak{d}_i, \mathfrak{d}_i'$ $(i = 1, \ldots, n-1)$, insbesondere $\mathfrak{d}_{n-1}, \mathfrak{d}_{n-1}'$ Teiler von D_0' sind.

Beweis von 1°. Bezeichne $\mathfrak{h}_i$ $(i=1,\ldots,n)$ die K_i zugeordnete Idealgruppe in Ω. Mit $\mathfrak{h}_i'$ bezeichnen wir das Konjugierte von $\mathfrak{h}_i$ in Ω. Mit $\mathfrak{h}_i$ zusammen ist auch $\mathfrak{h}_i'$ eine Weber—Takagische Idealgruppe in Ω. Für sie ist $\tilde{m}=mp_\infty$ ein gemeinsamer Erklärungsmodul. Bezeichne $\mathfrak{a}$ ein zu $\mathfrak{m}$ primes Ideal in $\mathfrak{h}_i$ und $\mathfrak{a}'$ das Konjugierte von $\mathfrak{a}$ (in Ω). Da $\mathfrak{a}\mathfrak{a}'$ rational und prim zu m ist, so gilt

$$\mathfrak{a}\mathfrak{a}' \in H_m \subseteq H \subseteq \mathfrak{h}_i.$$

Hieraus folgt $\mathfrak{a}' \in \mathfrak{h}_i'$, $\mathfrak{h}_i \subseteq \mathfrak{h}_i'$. Nach Übergang zum Konjugierten folgt

$$\mathfrak{h}_i' = \mathfrak{h}_i. \tag{77}$$

Dies bedeutet, daß K_i (absolut) Galoissch ist.

Wir bezeichnen mit T_n einen erzeugenden Automorphismus von $K_n|\Omega$, wofür also (54), (50_1) gelten. Bezeichnen wir mit $\mathfrak{P}$ einen Primidealfaktor von D in K_n. Wegen $(D,m)=1$ ist die Trägheitsgruppe von $\mathfrak{P}$ in $K_n|\Omega$ und in $K_n|P$ von der Ordnung 1 bzw. 2. Wir bezeichnen mit U_n das von 1 verschiedene Element der letztgenannten Trägheitsgruppe. Mit diesem gelten dann (49) und (50_2). Um auch (50_3) zu zeigen, schreiben wir T_n als Artinsches Symbol

$$T_n = \left(\frac{K_n|\Omega}{\mathfrak{a}}\right)$$

mit einem passenden Ideal $\mathfrak{a}$ in Ω. Da U_n ein erzeugender Automorphismus für Ω ist, so ist $U_n\mathfrak{a}=\mathfrak{a}'$ das Konjugierte von $\mathfrak{a}$, ferner gilt

$$U_n T_n U_n^{-1} = \left(\frac{U_n K_n|U_n\Omega}{U_n\mathfrak{a}}\right) = \left(\frac{K_n|\Omega}{\mathfrak{a}'}\right) = \left(\frac{K_n|\Omega}{\mathfrak{a}\mathfrak{a}'}\right) T_n^{-1} = T_n^{-1},$$

wobei berücksichtigt wurde, daß $\mathfrak{a}\mathfrak{a}'$ rational ist, also in $\mathfrak{h}_n$ liegt. Wir haben die Richtigkeit von (50_3) bewiesen. Die übrigen Behauptungen in 1° sind eine unmittelbare Folgerung aus den bekannten Eigenschaften der Gruppe $\{T_n, U_n\}$ und der Theorie von Galois.

Beweis von 2°. Da die Quadrate der Primidealfaktoren von D in Ω rational sind, also in H liegen, so liegen selbst die gesagten Primideale je in einer Klasse A. Hieraus folgt nach [8] Satz 3 die Richtigkeit von 2°.

Beweis von 3°, 4° und 6°. Da $\mathfrak{G}(K_i|A_{i-2})$ die Diedergruppe 8-ter Ordnung ist und diese nur eine normale Untergruppe 2-ter Ordnung hat, so gibt es zwischen A_{i-2} und K_i nur einen Körper, der Galoissch und vom Grade 4 über A_{i-2} ist $(i=2,\ldots,n)$. Dieser muß K_{i-1} sein, folglich ist $A_i|A_{i-2}$ nicht Galoissch. Andererseits ist $A_{i-1}|A_{i-2}$ Galoissch, somit ist $A_i, \bar{A}_i$ nach (53_3) ein volles System konjugierter Körper über A_{i-2}.[36] Hiernach ist

$$D_{\bar{A}_i|A_{i-1}} = D'_{A_i|A_{i-1}} \qquad (i=2,\ldots,n), \tag{78}$$

wobei der Strich „′" das Übergehen zum Konjugierten in $A_{i-1}|A_{i-2}$ bezeichnet.

[36] Dies beweist auch (68_2).

Da die Diskriminante eines relativquadratischen Körpers das Quadrat der Differente ist, so gilt nach HILBERT

(79) $$D_{K_{i+1}|A_{i+1}} D_{A_{i+1}|A_i} = D_{K_{i+1}|K_i} D_{K_i|A_i} \qquad (i=0,\ldots,n-1).$$

Wegen $K_{i+1} = K_i A_{i+1}$ ist

$$D_{K_{i+1}|A_{i+1}} | D_{K_i|A_i},$$

ferner ist hier die rechte Seite nach (51) ein Teiler von D. Hieraus und aus (79) folgt, daß

$$D_{A_{i+1}|A_i} D^{-1}_{K_{i+1}|K_i}$$

ganz und ein Teiler von D ist. Indem wir also (71) und (56) als Definition von $\mathfrak{m}_i$ und $\mathfrak{d}_i$ betrachten, so bedeutet das gewonnene, daß $\mathfrak{d}_i$ ganz und ein Teiler von D ist. Andererseits ist $\mathfrak{m}_i$ nach (71) ein Teiler von $D_{K_n|\Omega}$, also ein Teiler einer Potenz von m. Da ferner m ungerade, also $\mathfrak{m}_i$ zu 2 prim ist, und $K_{i+1}|K_i$ den Grad 2 hat, so folgt aus (71), daß $\mathfrak{m}_i$ sogar ein Teiler von m sein muß. Somit sind $\mathfrak{d}_i, \mathfrak{m}_i$ wegen $(D, m) = 1$ schon durch (56) allein eindeutig definiert als ganze Ideale in A_i.

Da K_i, K_{i+1} beide Galoissch sind, so folgt aus (71) auch, daß $\mathfrak{m}_i$ selbstkonjugiert ist.

Hieraus und aus (56), (78) folgt die Richtigkeit von (70_2).

Nach der Führer-Diskriminantenformel gilt

(80) $$D_{K_n|\Omega} = \prod_\chi f_\chi,$$

wobei χ die von 1 verschiedenen Charaktere von $\mathfrak{H}/\mathfrak{h}_n$ durchläuft und f_χ den endlichen Teil des Führers derjenigen Idealgruppe $\mathfrak{h}_\chi$ bezeichnet, die aus den die Gleichung $\chi(X) = 1$ befriedigenden Nebengruppen von $\mathfrak{h}_n$ besteht. Da unter den χ genau 2^{i-1} von der Ordnung 2^i sind $(i = 1, \ldots, n)$ und für sie $\mathfrak{h}_\chi = \mathfrak{h}_i, f_\chi = f_i$ gilt, wobei f_i den endlichen Teil des Führers von $\mathfrak{h}_i$ bezeichnet, so haben wir nach (80)

(81) $$D_{K_n|\Omega} = f_1 f_2^2 f_3^{2^2} \ldots f_n^{2^{n-1}}.$$

Andererseits gilt nach HILBERT

$$D_{K_n|\Omega} = N_{K_{n-1}|\Omega}(D_{K_n|K_{n-1}}) \cdot D^2_{K_{n-1}|\Omega}.$$

Wegen (71) und der Selbstkonjugiertheit von $\mathfrak{m}_{n-1}$ folgt hieraus

(82) $$D_{K_n|\Omega} = \mathfrak{m}_{n-1}^{2^{n-1}} D^2_{K_{n-1}|\Omega}.$$

Dies und (81) ergeben

(83) $$\mathfrak{m}_{n-1}^{2^{n-1}} = (f_1 f_2^2 f_3^{2^2} \ldots f_{n-1}^{2^{n-2}})^{-1} f_n^{2^{n-1}}.$$

Nun folgt aus (77), daß die f_i selbstkonjugierte Ideale in Ω sind. Außerdem sind sie Teiler von m, deshalb sind sie ganze rationale Teiler von m. Da ferner wegen $\mathfrak{h}_1 \supset \ldots \supset \mathfrak{h}_n$ die Teilbarkeitsbeziehungen

$$f_1 | \cdots | f_n$$

gelten, so läßt sich

$$f_i = m_1 \cdots m_i \qquad (i = 1, \ldots, n) \tag{84}$$

setzen mit eindeutig bestimmten primären Teilern $m_1, \ldots, m_n$ von m, für die auch (58) gilt. (Wir haben berücksichtigt, daß es auf das Vorzeichen von f_i nicht ankommt.) Nach Einsetzung von (84) in (83) entsteht

$$\mathfrak{m}_{n-1}^{2^{n-1}} = m_1 m_2^2 m_3^{2^2} \ldots m_n^{2^{n-1}}.$$

Da die Faktoren der rechten Seite wegen (58) paarweise relativ prim sind, so sind sie mit der linken Seite zusammen lauter 2^{n-1}-te Potenzen von Idealen in A_{n-1}. Somit folgt die Richtigkeit von (57) für $i = n-1$, also auch für die übrigen i.

Ähnlich zu (82) entsteht

$$D_{K_{i+1}|A_i} = \mathfrak{m}_i^2 D_{K_i|A_i}^2 \qquad (i = 0, \ldots, n-1).$$

Andererseits ergibt sich nach (53) aus der Führer-Diskriminantenformel

$$D_{K_{i+1}|A_i} = D_{K_i|A_i} D_{A_{i+1}|A_i} D_{\bar{A}_{i+1}|A_i}.$$

Aus beiden folgt

$$D_{A_{i+1}|A_i} D_{\bar{A}_{i+1}|A_i} = \mathfrak{m}_i^2 D_{K_i|A_i} \qquad (i = 0, \ldots, n-1). \tag{85}$$

Dies lautet für $i = 0$ wegen (57):

$$D_{A_1} D_{\bar{A}_1} = m_1^2 D.$$

Da $A_1, \bar{A}_1$ quadratisch sind und m_1 primär ist, so folgen hieraus (55), (68_1), ferner (59_1) und (70_1).

Aus (56), (78) und dem Fall $i > 0$ von (85) folgt wieder wegen der Selbstkonjugiertheit von $\mathfrak{m}_i$:

$$\mathfrak{d}_i \mathfrak{d}_i' = D_{K_i|A_i} \qquad (i = 1, \ldots, n-1). \tag{86}$$

Andererseits folgt aus (71), (79), (85)

$$D_{K_{i+1}|A_{i+1}} D_{\bar{A}_{i+1}|A_i}^{-1} = \mathfrak{m}_i^{-1} \qquad (i = 0, \ldots, n-1).$$

Also gilt nach (70) (wegen $\mathfrak{m}_0 = m_1$)

$$D_{K_1|A_1} = D_0', \quad D_{K_{i+1}|A_{i+1}} = \mathfrak{d}_i' \qquad (i = 1, \ldots, n-1).$$

Dies und (86) beweisen (59_2) und (59_3).

Wäre (60) falsch, so gäbe es nach (56), (78) ein Primideal $\mathfrak{p}$ in A_i, das in beiden Körpern $A_{i+1}, \bar{A}_{i+1}$ verzweigt und dabei nach (59) ein Teiler von D ist. Andererseits ist $\mathfrak{p}$ in $K_{i+1}|A_i$ nicht vollverzweigt, weshalb in diesem Körper die Trägheitsgruppe jedes Primidealfaktors von $\mathfrak{p}$ von der zweiten Ordnung, also sein Trägheitskörper gleich K_i ist. Das ist aber unmöglich, da die Primidealfaktoren von D in $K_{i+1}|K_i$ nicht verzweigen. Dieser Widerspruch beweist (60).

Aus (59) folgt offenbar (61).

Der Fall $i=1$ von (62) ist dasselbe wie (59_2). Für $i=2,\ldots,n-1$ folgt aus (59_3).

$$N_{A_i}\mathfrak{d}_i = N_{A_{i-1}}(N_{A_i|A_{i-1}}\mathfrak{d}_i) = N_{A_{i-1}}(\mathfrak{d}_i\mathfrak{d}_i') = N_{A_{i-1}}\mathfrak{d}_{i-1}' = N_{A_{i-1}}\mathfrak{d}_{i-1}.$$

Dies ergibt mit Induktion die Richtigkeit von (62) allgemein. Somit haben wir 3^0, 4^0 und 6^0 bewiesen.

Beweis von 5^0. Wir haben (68) schon oben bewiesen. Aus (53), (55), (63), (68) folgt offenbar auch (69).

Es muß

(87) $$K_i = A_i(\sqrt{\alpha_i\alpha_i'}) \qquad (i=1,\ldots,n-1)$$

gelten, weil die rechte Seite nach (53), (63), (68_2) ein Unterkörper von K_{i+1}, quadratisch über A_i und von A_{i+1}, A_{i+1} verschieden ist. Da andererseits $\alpha_i\alpha_i' \in A_{i-1}$ ist, so folgt aus (87), daß

(88) $$A_{i-1}(\sqrt{\alpha_i\alpha_i'}) \qquad (i=1,\ldots,n-1)$$

quadratisch über A_{i-1} ist. Dabei ist (88) wegen (87) von A_i verschieden, muß also nach (53) mit einem der Körper (vgl. (51), (68))

(89) $$K_{i-1} = A_{i-1}(\sqrt{D}), \quad A_i = A_{i-1}(\sqrt{\alpha_{i-1}'}) \qquad (i=1,\ldots,n-1)$$

übereinstimmen, wobei für einen Augenblick $\alpha_0' = D_0'$ gesetzt wurde.

Zuerst nehmen wir an, daß (88) für ein i $(=1,\ldots,n-1)$ mit (89_1) übereinstimmt. Das bedeutet

$$\alpha_i\alpha_i' \underset{(2)}{=} D \text{ (in } A_{i-1}).$$

Wegen $\sqrt{D} \in K_{i-1}$, $A_{i-1} \subset K_{i-1}$ folgt hieraus

$$\sqrt{\alpha_i}\sqrt{\alpha_i'} \in K_{i-1}.$$

Wegen der Verschiedenheit der Körper A_{i+1}, A_{i+1} ist nach (63), (68) gewiß $\alpha_i' \neq \alpha_i$, weshalb α_i außerhalb von A_{i-1} liegt. Wegen $A_{i-1} = K_{i-1} \cap A_i$ und $\alpha_i \in A_i$ muß α_i sogar außerhalb von K_{i-1} liegen. Bezeichnet also T ein erzeugendes Element von $\mathfrak{G}(K_{i+1}|K_{i-1})$, so gilt

$$T\alpha_i \neq \alpha_i.$$

Andererseits sind α_i, α_i' konjugiert über A_{i-1}, folglich auch über K_{i-1}. Somit gilt

$$T\alpha_i = \alpha_i'.$$

Hieraus folgt $T\sqrt{\alpha_i} = \pm\sqrt{\alpha_i'}$, also nach obigem

$$\sqrt{\alpha_i}\cdot T\sqrt{\alpha_i} \in K_{i-1}.$$

Dann bleibt die linke Seite bei Anwendung von T unverändert, somit gilt

$$T^2\sqrt{\alpha_i} = \sqrt{\alpha_i}.$$

Hiernach liegt $\sqrt{\alpha_i}$ in K_i. Dies steht aber in einem Widerspruch mit (69),

woraus folgt, daß (88) nicht mit (89_1), sondern mit (89_2) übereinstimmt. Dies bedeutet die Richtigkeit von (64_2), (64_3). Da auch (64_1) richtig ist, so haben wir zum vollständigen Beweis von 5° nur noch (65) bis (67) zu bestätigen.

Hiervon wird uns der Beweis von (67) wenig Mühe machen. Da nämlich α_0 rational ist, so ist (67) für $i=0$ trivial. Für den Fall $i>0$ gilt nach (69_2)

$$\mathsf{K}_{i+1}=\mathsf{K}_i(\sqrt{\alpha_i}).$$

Folglich gilt auch

$$\mathsf{K}_{i+1}=\mathsf{K}_i(\sqrt{T_n\alpha_i}).$$

Aus beiden folgt

$$\sqrt{T_n\alpha_i}\,(\sqrt{\alpha_i})^{-1}\in\mathsf{K}_i,$$

also $T_n\alpha_i \underset{(2)}{=} \alpha_i (\text{in } \mathsf{K}_i)$. Somit haben wir (67) bewiesen.

Wenn $\mathfrak{d}_i$ also auch $\mathfrak{d}_i\mathfrak{m}_i$ zu 2 prim ist, so folgt aus (56), (63) sofort die Richtigkeit von (65), (66). Es ist nur noch der Fall übrig, daß $\mathfrak{d}_i$ nicht zu 2 prim ist. Zum vorigen ähnlichen Schluß fehlt jetzt nur der Nachweis, daß $\alpha_i\mathfrak{d}_i^{-1}$ alle Primidealfaktoren von 2 in A_i zur geraden Potenz enthält. Da $\alpha_0=D_0m_1$, $\mathfrak{d}_0=D_0$ gelten und m_1 ungerade ist, so sind wir mit dem Fall $i=0$ fertig. Nachher sei $i>0$. Wegen der Annahme haben wir es nach (62) mit einer durch 2 teilbaren D_0' zu tun. Folglich gilt jetzt

$$2=\mathfrak{p}\mathfrak{p}'\mathfrak{q}_1^2\ldots\mathfrak{q}_k^2, \tag{90}$$

wobei $\mathfrak{p},\mathfrak{p}',\mathfrak{q}_1,\ldots,\mathfrak{q}_k$ verschiedene Primideale in A_i und $\mathfrak{p},\mathfrak{p}'$ konjugiert bezüglich A_{i-1} sind (vgl. die Bemerkung bei (76)). Kein $\mathfrak{q}_j$ geht in $\mathfrak{d}_i$ auf, denn im Fall $\mathfrak{q}_j\,|\,\mathfrak{d}_i$ wäre $\mathfrak{q}_j$ wegen (56) in $\mathsf{A}_{i+1}\,|\,\mathsf{A}_i$ verzweigt, somit hätte 2 wegen (90) einen vierfachen Primidealfaktor in A_{i+1}, das aber wegen 2° unmöglich ist. Folglich dürfen wir annehmen, daß $\mathfrak{p}\,|\,\mathfrak{d}_i$ ist. Aus (60) folgt dann $\mathfrak{p}\nmid\mathfrak{d}_i'$ also $\mathfrak{p}'\nmid\mathfrak{d}_i$. Hiernach ist unter allen Primidealen auf der rechten Seite von (90) nur $\mathfrak{p}$ ein Teiler von $\mathfrak{d}_i$. Hieraus und aus (56), (63) folgt

$$\alpha_i \underset{(2)}{=} \mathfrak{p}^s\mathfrak{a} \ (\text{in } \mathsf{A}_i)$$

mit einer ganzen rationalen Zahl s $(=0, 1)$ und einem zu 2 primen Ideal $\mathfrak{a}$ in A_i. Andererseits sind $\alpha_1,\ldots,\alpha_{i-1}$ Quadratzahlen in A_i, weshalb aus (64)

$$N_{\mathsf{A}_i}\alpha_i \underset{(2)}{=} D_0'm_1 \ (\text{in } \mathsf{A}_i)$$

folgt. Dies und (62) ergeben

$$N_{\mathsf{A}_i}(\alpha_i\mathfrak{d}^{-1}) \underset{(2)}{=} m_1 \ (\text{in } \mathsf{A}_i).$$

Da in $\alpha_i\mathfrak{d}_i^{-1}$ kein Primideal außer $\mathfrak{p}$ auf der rechten Seite von (90) zur ungeraden Potenz enthalten und $N_{\mathsf{A}_i}\mathfrak{p}=2$ ist, so folgt hieraus, daß $\alpha_i\mathfrak{d}^{-1}$ alle Primidealfaktoren von 2 in A_i zur geraden Potenz enthält. Somit haben wir den Beweis von 5° beendet.

Beweis von 7°. Wir fangen es mit dem zweiten (auf $n=1$ bezüglichen) Teil von 7° an. Zuerst wollen wir zeigen, daß jeder durch (74) gegebene Körper K_1^* wirklich ein K_1' ist. Da in (74) die Ersetzung von D^* durch DD^{*} [1]

unwesentlich ist, so dürfen wir uns auf den Fall $2 \nmid D^*$ beschränken. Man sieht leicht, daß dann

$$D_{K_1^* | \Omega} = m^*$$

ist. Wird also die dem Körper K_1^* zugeordnete Idealgruppe in Ω mit $\mathfrak{h}$ bezeichnet, so folgt, daß $\mathfrak{h}$ den Führer m^* oder $m^* p_\infty$ hat. Deshalb gilt $H_{m^*} \subseteqq \mathfrak{h}$. Da ferner $\mathfrak{h}$ in der Gruppe aller zu $m p_\infty$ primen Ideale von Ω den Index 2 hat, so gilt sogar $H \subseteqq \mathfrak{h}$. Somit ist K_1^* wirklich ein K_1'.

Andererseits zeigt (69_1), daß umgekehrt jedes K_1' unter den K_1^* in (74) vorkommt.

Wir haben noch unter den K_1^* in (74) die verschiedenen auszusuchen und ihre Zahl zu bestimmen. Wir haben schon bemerkt, daß sie je zu zweien gleich sind, aber es ist auch klar, daß die übriggebliebenen verschieden sind. Da ferner die Anzahl der K_1^* in (74) offenbar $2^t - 2$ ist, so gibt es genau $2^{t-1} - 1$ verschiedene K_1^*.

Ein Vergleich mit (55) zeigt, daß für K_1^*, A_1^* eben $m_1 = m^*$, $\mathfrak{d}_0 = D^*$ ausfällt. Somit haben wir den zweiten Teil von 7^0 bewiesen.[37]

Um den ersten (auf $2 \leqq n \leqq \nu$ bezüglichen) Teil von 7^0 zu beweisen, bestimmen wir zuerst die Anzahl aller K_n' über dem festen K_{n-1}. Diese Zahl ist genau so groß, wie die Zahl der zyklischen Untergruppen der Ordnung 2^n von $\mathfrak{H}$, die eine feste Untergruppe von der Ordnung 2^{n-1} enthalten, sie ist also gleich $2^{e_1 - 1}$. Da nach (18) $e_1 = t - 1$ ist, so ist die gefragte Anzahl gleich 2^{t-2}.

Andererseits ist die Anzahl der Zahlen $D^* m^*$ in (72) gleich 2^t. Ferner ist die auf die Verschiedenheit der Körper (72) bezügliche Behauptung offenbar richtig. Um also zu zeigen, daß die verschiedenen Körper K_n^* in (72) mit den obigen K_n' identisch sind, haber wir nur noch zu beweisen, daß jedes K_n^* ein K_n' ist. Dies stimmt, denn K_n^* ist nach (69_2) ein Unterkörper von

$$K_n \cdot \Omega(\sqrt{D^* m^*}),$$

der zyklisch und vom Grad 2^n über Ω ist.

Wir haben noch (73) zu beweisen. Hierzu setzen wir

$$r = m_1 \cdots m_{n-1}.$$

Nach (57), (71) ist r ein Idealquadrat in K_{n-1}, dagegen sind die Primzahlfaktoren von $\frac{m}{r}$ unverzweigt in K_{n-1}. Wegen (57), (69), (71) gilt also

$$\alpha_{n-1} \underset{(2)}{=} m_n \mathfrak{a} \quad (\text{in } K_{n-1})$$

mit einem zu $\frac{m}{r}$ primen Ideal $\mathfrak{a}$. Entsprechend gilt wegen (72) und $(D, m) = 1$

$$m^* \alpha_{n-1} \underset{(2)}{=} m_n^* \mathfrak{b} \quad (\text{in } K_{n-1})$$

[37] Durch obiges wurde auch der noch fehlende Beweis der ersten Hälfte von Satz 1 nachgeholt.

mit einem zu $\frac{m}{r}$ primen Ideal $\mathfrak{b}$. Aus beiden folgt

$$m_n^* \underset{(2)}{=} m^* m_n \mathfrak{a} \mathfrak{b} \quad (\text{in } K_{n-1}).$$

Spaltet man die zu $\frac{m}{r}$ primen Faktoren ab, so bekommt man

$$m_n^* \underset{(2)}{=} \frac{m^*}{(m^*, r)} m_n \quad (\text{in } K_{n-1}),$$

wobei beide Seiten unverändert als Ideale in K_{n-1} aufzufassen sind. Da die linke Seite und beide Faktoren der rechten Seite Teiler von $\frac{m}{r}$ sind, so folgt aus obigem Grunde, daß diese Gleichung auch in P gilt. So entsteht eben (73_1).

Um auch (73_2) zu beweisen, bemerken wir, das nach (56), (63) die Diskriminante von

$$A_{n-1}(\sqrt{\alpha_{n-1}}) \mid A_{n-1}$$

durch $\mathfrak{d}_{n-1}$ teilbar ist. Deshalb ist die Diskriminante $\mathfrak{d}_{n-1}^* \mathfrak{m}_{n-1}^*$ von

$$A_{n-1}(\sqrt{D^* m^* \alpha_{n-1}}) \mid A_{n-1}$$

(vgl. (56)) jedenfalls durch $(DD^{*-1}, \mathfrak{d}_{n-1})$ teilbar, also

$$(DD^{*-1}, \mathfrak{d}_{n-1}) \mid \mathfrak{d}_{n-1}^*.$$

Andererseits müssen die Körper

$$\bar{A}_n = A_{n-1}(\sqrt{\alpha'_{n-1}}), \quad A_{n-1}(\sqrt{D\alpha_{n-1}})$$

gleich sein, da beide zwischen A_{n-1} und K_n liegen, ferner von $A_n = A_{n-1}(\sqrt{\alpha_{n-1}})$ verschieden sind. Da hiernach (vgl. (70_2)) die Diskriminante von

$$A_{n-1}(\sqrt{D\alpha_{n-1}}) \mid A_{n-1}$$

durch $\mathfrak{d}'_{n-1}$ teilbar ist, so folgt ähnlich wie vorher

$$(D^*, \mathfrak{d}'_{n-1}) \mid \mathfrak{d}_{n-1}^*.$$

Wir haben gewonnen, daß die rechte Seite von (73_2) ein Teiler der linken Seite ist. Beide Seiten haben aber nach dem Fall $i = n-1$ von (59_3) (angewendet auf A_n und A_n^*) die gleiche Norm in $A_{n-1} \mid A_{n-2}$ (nämlich $\mathfrak{d}'_{n-1}$), folglich ist (73_2) richtig. Somit haben wir den Beweis von Satz 5 beendet.

§ 6. Die Konstruktion der Ringklassenkörper K_n

Hier wollen wir die Körper K_n konstruieren. Wie gesagt, das wird ein wichtiger Beitrag zur Sicherung der Anwendbarkeit der vorigen Sätze 1 bis 4.

Insbesondere haben wir die sämtlichen K_1 durch (74) schon angegeben. Deshalb werden wir von einem gegebenen K_n $(n \geqq 1)$ ausgehen, über dem mindestens ein K_{n+1} existiert, und konstruieren dann einen dieser Körper. Das genügt vollkommen, denn nach (72) werden hierdurch schon alle K_{n+1} über

K_n bekannt, somit werden wir durch die Lösung der gesagten Aufgabe imstande sein, nach und nach überhaupt alle $K_1, K_2, \ldots$ zu konstruieren. Die Lösung der Aufgabe wird im Prinzip im folgenden Satz 6 enthalten sein, der aber im anschließenden Zusatz seine Ergänzung findet, wo nämlich die Konstruktion auf die Lösung einer Folge einfacher Teilaufgaben zurückgeführt wird.

SATZ 6. *Es werde gegeben ein K_n $(n \geqq 1)$, über dem mindestens ein K_{n+1} existiert.*[38] *Man wähle einen der 2^n Unterkörper A_n $(\neq K_{n-1})$ von K_n vom Grade 2^n beliebig aus und übernehme gleichzeitig die im Satz 5 verwendeten Bezeichnungen für dieses Paar K_n, A_n. Dann gibt es eine Zahl α_n in A_n mit den Eigenschaften*[39]

(91) $$\alpha_n \alpha_n' \underset{(2)}{=} \alpha_{n-1}' \qquad (\text{in } A_{n-1}) \qquad (\alpha_0' = D_0' m_1),$$

(92) $$(\alpha_n) \underset{(2)}{=} \mathfrak{d}_n \mathfrak{m}_{n-1}^{2^{-1}}$$

(93) $$\alpha_n \underset{(2)}{\equiv} 1 \left(\bmod \frac{4}{(2, \mathfrak{d}_n)^2}\right) \qquad \Bigg\} (\text{in } A_n),$$

(94) $$\alpha_n \cdot T_n \alpha_n \underset{(2)}{=} 1 \qquad (\text{in } K_n),$$

wobei $\mathfrak{d}_n$ ein den Bedingungen

(95) $$\mathfrak{d}_n \mathfrak{d}_n' = \mathfrak{d}_{n-1}', \quad (\mathfrak{d}_n, \mathfrak{d}_n') = 1$$

genügendes (ganzes) Ideal in A_n ist und $\alpha_n', \mathfrak{d}_n'$ das Konjugierte von α_n bzw. $\mathfrak{d}_n$ in $A_n \mid A_{n-1}$ bezeichnet. Für jedes solche α_n ist $K_n(\sqrt{\alpha_n})$ ein $K_{n+1}(\supset K_n)$, und dabei ist $A_n(\sqrt{\alpha_n})$ ein von K_n verschiedener Unterkörper $A_{n+1}(\supset A_n)$ von K_{n+1}. Diesem Körperpaar K_{n+1}, A_{n+1} gehören $m_{n+1} = 1$ und $\mathfrak{d}_n$ im Sinne von Satz 5 zu.[40]

[38] Die notwendige und hinreichende Bedingungen dafür wurde in [8] Satz 3 angegeben. (Eine notwendige aber bei weitem nicht hinreichende Bedingung ist $n < \nu$.) Obiger Satz läßt sich auch dann anwenden, wenn man nicht weiß, ob über K_n ein K_{n+1} existiert, denn läßt sich die zu beschreibende Konstruktion ausführen, so wird durch sie — wie wir aus dem Beweis sehen werden — immer ein K_{n+1} über K_n geliefert. Natürlich ist aber viel besser, daß man die Frage der Existenz im voraus nachprüft, um sich mit dem Versuch einer eventuell unausführbaren Konstruktion keine überflüssige Mühe zu machen.

[39] In (92) ist die Behauptung mitenthalten, daß (wegen der Voraussetzung!) $\mathfrak{m}_{n-1}$ das Quadrat eines Ideals in A_n ist. Dieses Ideal wurde in (92) mit $\mathfrak{m}_{n-1}^{2^{-1}}$ bezeichnet. — Obige Existenzaussage werden wir sogar in folgender schärferer Form beweisen: Ist $\mathfrak{d}_n$ ein beliebiges ganzes Ideal in A_n mit (95), so gibt es ein $\alpha_n (\in A_n)$ mit (91) bis (94).

[40] Wegen $K_0 \subset \ldots \subset K_n \subset K_{n+1}$, $A_0 \subset \ldots \subset A_n \subset A_{n+1}$ (vgl. (48), (52)) können wir die im Satz 5 verwendeten Bezeichnungen auch für $n+1$ statt n als erklärt ansehen. Entsprechend haben wir also (als Analogon von T_n, U_n, A_n, $\bar{A}_n$, $\mathfrak{d}_{n-1}$, m_{n-1}, m_n, α_{n-1} usw.) die Bezeichnungen T_{n+1}, U_{n+1}, A_{n+1}, $\bar{A}_{n+1}$, $\mathfrak{d}_n$, $\mathfrak{m}_n$, m_{n+1}, α_n usw. zu verstehen. [Der Leser sieht, daß ein Teil dieser „neuen" Bezeichnungen auch schon oben im Satz 6 (in richtigem Sinne) benutzt wurde.] Erst nach dieser Bemerkung ist die obige Behauptung $m_{n+1} = 1$ sinnvoll geworden. Aus dieser Gleichung folgt nach (57), daß jetzt $\mathfrak{m}_n = \mathfrak{m}_{n-1}^{2^{-1}}$ gilt (vgl. [39]). — Wir bemerken wiederholt, daß wir uns im Satz 6 mit der Angabe *eines* $K_{n+1}(\supset K_n)$ begnügt haben, aber dann liefert (72) schon die sämtlichen $K_{n+1}(\supset K_n)$. Für diese kann m_{n+1} nach (73_1) jeder

BEMERKUNG. Die Bestimmung eines α_n mit den Eigenschaften (91) bis (95) scheint (im Fall $n \geqq 2$) eine schwierige Aufgabe zu sein, aber im folgenden Zusatz werden wir sehen, wie sich diese Aufgabe verhältnismäßig leicht lösen läßt. Erst im Besitz dieses Zusatzes wollen wir unsere Konstruktionsaufgabe als erledigt ansehen.

ZUSATZ. *Um eine Zahl* α_n *mit den im Satz 6 bei* (91) *bis* (95) *formulierten Eigenschaften zu bestimmen, genügt es den Fall* $n \geqq 2$, $D_0' \neq 1, -4$ *zu betrachten.*[41] *Man verfahre dann wie folgt.*

I. *Man setze*

(96) $$\alpha_{n-1} = \varkappa + \lambda \sqrt{\alpha_{n-1}} \qquad (\varkappa, \lambda \in \mathsf{A}_{n-2}),$$

löse die Gleichung

(97) $$\varrho^2 + D_0' m_1 \sigma^2 = 2\varkappa \tau^2 \qquad (\varrho, \sigma, \tau \in \mathsf{A}_{n-1};\ \tau \neq 0)$$

und berücksichtige, daß nach (64₂), (64₃)

(98) $$D_0 m_1 = \alpha_{n-1} \alpha_{n-1}' \zeta^2 \qquad (\zeta \in \mathsf{A}_{n-2})$$

gilt. Die Zahl

(99) $$\alpha_n = 2\varkappa\tau + (\varrho + \alpha_{n-1}' \sigma \zeta) \sqrt{\alpha_{n-1}}$$

liegt in A_n *und erfüllt die Bedingung* (91).

Teiler von $m(m_1 \ldots m_n)^{-1}$ sein, ferner gilt dann nach (57) allgemein $\mathfrak{m}_n = m_{n+1} \mathfrak{m}_{n-1}^{2^{-1}}$. Selbstverständlich läßt sich Satz 6 leicht so aussprechen, daß in ihm gleich ein beliebiges $\mathsf{K}_{n+1} (\supset \mathsf{K}_n)$ angegeben wird. Hierzu muß man nämlich bloß m_{n+1} als Faktor auf der rechten Seite von (92) hinzufügen.

[41] Ist nämlich $n = 1$, so hat man es mit einer verhältnismäßig sehr leichten Aufgabe zu tun, weshalb wir uns in diesem Fall mit Satz 6 begnügen können. Was den Ausschluß der Fälle $D_0' = 1, -4$ betrifft, hierüber bemerken wir folgendes. Man sieht aus (55), (68₁), daß bei Vertauschung von A_1 mit A_1 die Zahlen D_0, D_0' miteinander vertauscht werden. Wenn nunmehr $D \neq -4$ ist, so ist wegen $D_0 D_0' = D$ mindestens die eine der Zahlen D_0, D_0' von 1 und -4 verschieden, somit läßt sich A_n so wählen, daß $D_0' \neq 1, -4$ ausfällt, weshalb jetzt diese Annahme keine wesentliche Einschränkung bedeutet. Es bleibt nur $D = -4$ als einziger Ausnahmefall übrig, wo nämlich Ω der Gaußsche Zahlkörper $\mathsf{P}(\sqrt{-1})$ ist. Auf diesen Fall läßt sich das im Zusatz anzugebende Konstruktionsverfahren nicht ohne weiteres anwenden, das ist aber jetzt auch nicht nötig, denn man kann sich in diesem Fall mit Satz 6 zufriedenstellen. Man treffe jetzt nämlich die Wahl $D_0 = -4$, $D_0' = 1$, was nach dem Gesagten möglich ist. Dann ist nach (59₂), (59₃) $\mathfrak{d}_{n-1}' = 1$, also nach (95₁) auch $\mathfrak{d}_n = 1$, weshalb sich die Bedingungen (91) bis (95) von Satz 6 auf

$$\alpha_n \alpha_n' \underset{(2)}{\equiv} \alpha_{n-1}' \qquad (\text{in } \mathsf{A}_{n-1}),$$

$$\left.\begin{aligned} (\alpha_n) &\underset{(2)}{\equiv} \mathfrak{m}_{n-1}^{2^{-1}} \\ \alpha_n &\underset{(2)}{\equiv} 1 \pmod 4 \end{aligned}\right\} \qquad (\text{in } \mathsf{A}_n),$$

$$\alpha_n . T_n \alpha_n \underset{(2)}{\equiv} 1 \qquad (\text{in } \mathsf{K}_n)$$

reduzieren. Der Leser kann sich die Änderungen durchführen, mit denen der Zusatz auch auf diesen, viel einfacheren Fall anwendbar wird. Übrigens beabsichtigen wir auf diesen interessanten Ausnahmefall $D = -4$ an anderer Stelle zurückzukommen.

II. *Man ändere die eben gefundene Zahl α_n durch Hinzufügung eines Faktors in A_{n-1} so ab, daß das „neue“ α_n auch den Bedingungen* (92), (93), (95) *genügt.*

III. *Man nehme an, daß für die bisher gefundene Lösung α_n von* (91), (92), (93), (95) *mit einem festen i $(1 \leqq i \leqq n-1)$ auch noch*

$$\alpha_n \cdot T_n^{2^i} \alpha_n \underset{(2)}{=} 1 \qquad (\text{in } \mathsf{K}_n) \tag{100}$$

gilt. Man setze

$$\mu = \sqrt{\alpha_n \cdot T_n^{2^i} \alpha_n} \qquad (\in \mathsf{K}_n), \tag{101}$$

$$j = 2^{n-i}, \tag{102}$$

$$\mu_0 = \alpha_n \cdot T_n^{2^i} \alpha_n, \quad \mu_a = \mu_{a-1} \cdot T_n^{(a-1)2^{i-1}} (\alpha_n^{-1} \mu) \qquad (a = 1, \ldots, j), \tag{103}$$

$$\omega = S_{\mathsf{K}_n | \mathsf{K}_{n-1}} (\mu_0 + 2\mu_1 + \cdots + 2\mu_{j-1} + \mu_j). \tag{104}$$

Diese Zahl ω liegt in A_{i-1}. Man wähle das Vorzeichen von μ so, daß es eine Zahl ω_i in A_i mit

$$\left.\begin{aligned} &\omega_i \omega_i' \underset{(2)}{=} \omega && (105)\\ &(\omega_i) \underset{(2)}{=} 1 && (106)\\ &\omega_i \underset{(2)}{\equiv} 1 \pmod 4 && (107)\end{aligned}\right\} (\text{in } \mathsf{A}_n)$$

gibt, wobei ω_i' das Konjugierte von ω in $\mathsf{A}_i | \mathsf{A}_{i-1}$ bezeichnet. Wenn man nun α_n mit ω_i multipliziert und dieses Produkt wieder mit α_n bezeichnet, so behalten (91) *bis* (93) *ihre Gültigkeit (mit unverändertem $\mathfrak{d}_n$), außerdem wird* (100) *mit $i-1$ statt i gültig.*

All' dieses ist ausführbar. Da ferner (100) *insbesondere für $i = n-1$ eine Folgerung von* (91) *ist,*[42] *so läßt sich* III *der Reihe nach mit $i = n-1, \ldots, 1$ anwenden. Da* (100) *für $i = 0$ mit* (94) *identisch ist, so ist das Resultat eine Zahl α_n in A_n mit den im Satz* 6 *geforderten Eigenschaften* (91) *bis* (95).

Bemerkung. Man erstrecke die Definition (103) auch auf $a = j+1, \ldots, 2j-1$. Dann gilt, wie wir das zeigen werden,

$$\omega \alpha_n \cdot T_n^{2^{i-1}} \alpha_n = (\mu_0 + \cdots + \mu_{2j-1})^2. \tag{108}$$

Andererseits schreibe man (105) in der Form

$$\omega_i \cdot T_n^{2^{i-1}} \omega_i = \omega \gamma^2 \qquad (\gamma \in \mathsf{A}_{i-1}).$$

Durch Multiplikation entsteht

$$\omega_i \alpha_n \cdot T_n^{2^{i-1}} (\omega_i \alpha_n) = \gamma^2 (\mu_0 + \cdots + \mu_{2j-1})^2.$$

[42] Offenbar ist nämlich $\alpha_n = T_n^{2^{n-1}} \alpha_n$, ferner ist α'_{n-1} wegen (69_2) eine Quadratzahl in K_n.

Der Vergleich mit (101) zeigt, daß bei der Wiederholung von III mit $i-1$ statt i das „neue“ μ gleich
$$\pm\gamma(\mu_0+\cdots+\mu_{2j-1})$$
wird. Diese Bemerkung erleichtert die Anwendung des Zusatzes.[43]

Beweis von Satz 6. Die Lösbarkeit von (91) bis (95) ist eine Folgerung der angenommenen Existenz von K_{n+1} und von Satz 5. Wendet man nämlich diesen mit $n+1$ statt n an, so entstehen (91), (93), (94), (95) der Reihe nach als der Fall $i=n$ von (64_3), (66), (67) bzw. (59_3), (60). Statt der noch fehlenden Gleichung (92) bekommt man dagegen aus (65) sogar die allgemeinere Gleichung
$$(\alpha_n)\underset{(2)}{=}\mathfrak{d}_n\mathfrak{m}_n \qquad (\text{in } \mathsf{A}_n).$$

Aus dieser entsteht nämlich (92), wie wir das aus (57) sehen, als der Spezialfall $m_{n+1}=1$. Da nach (73_1) aus der Existenz eines $\mathsf{K}_{n+1}(\supset\mathsf{K}_n)$ auch die eines $\mathsf{K}_{n+1}(\supset\mathsf{K}_n)$ mit $m_{n+1}=1$ folgt, so haben wir die Lösbarkeit von (91) bis (95) ausgewiesen. Das ist sogar gleich in der schärferen Form geschehen, daß man dabei für $\mathfrak{d}_n$ jede Lösung von (95) vorschreiben darf (vgl. die zweite Hälfte von[39]).

Nunmehr setzen wir (91) bis (95) voraus. Wir bezeichnen

$$A=\mathsf{K}_n(\sqrt{\alpha_n}),\quad \mathsf{B}=\mathsf{A}_n(\sqrt{\alpha_n}). \tag{109}$$

Vor allem zeigen wir $A\neq\mathsf{K}_n$. Im anderen Fall wäre α_n eine Quadratzahl in K_n. Da $\mathsf{K}_n=\mathsf{A}_n\bar{\mathsf{A}}_1$, also nach ($68_1$)
$$\mathsf{K}_n=\mathsf{A}_n(\sqrt{c}) \qquad (c=D_0'm_1)$$
ist, so folgt das Bestehen einer Gleichung
$$\alpha_n=(\alpha+\beta\sqrt{c})^2 \qquad (\alpha,\beta\in\mathsf{A}_n).$$

[43] Folgendes soll bemerkt werden. „Theoretisch“ kann man sich mit Satz 6 zufriedenstellen, „praktisch“ ist auch der Zusatz wichtig. D. h. wenn man z. B. die asymptotische Formel für die Anzahl der Fälle aufstellen will, in denen $e_1,\ldots,e_k$ vorgegebene Werte haben bzw. Ringeinheiten von negativer Norm existieren (zwei Probleme, mit denen wir uns — wie gesagt — an anderer Stelle beschäftigen wollen), so kommt man mit Satz 6 (ohne den Zusatz) aus. Will man dagegen für ein (numerisch) gegebenes Paar d, m die $e_1,\ldots,e_r$ berechnen oder über die Lösbarkeit von $x^2-dm^2y^2=-1$ entscheiden, so hat man auch den Zusatz heranzuziehen. — Trotz der Länge des Zusatzes kann man mit ihm sehr gut arbeiten. In der Hauptsache kommt es nämlich auf eine Lösung von (97) an, denn die Ausführung der übrigen Rechnungen ist augenscheinlich eine leichtere Aufgabe. Auch die Auffindung einer Lösung der (quadratischen) Gleichung (97) ist nicht schwer, denn man kann zur Lösung wegen ihrer Homogeneität die bekannten leichten Kunstgriffe verwenden. (Übrigens ist der Teil I des Zusatzes entbehrlich, denn (91) läßt sich auch unmittelbar gut lösen.) Wir machen hier auf einen durch unseren Satz 6 und Zusatz beseitigten Fehler in der Arbeit von Reichardt [22] (Seite 81, Zeilen 6 bis 8) aufmerksam, der in der Behauptung besteht, daß Satz 6 (im von Reichardt betrachteten Fall $m=1$), auch ohne (94) gültig wäre.

Da $\sqrt{c}$ nicht in A_n liegt, so folgt hieraus $\alpha\beta = 0$. Hiernach ist α_n gleich α^2 oder $c\beta^2$, somit ist $\alpha_n \alpha_n'$ in beiden Fällen eine Quadratzahl in A_{n-1}. Nach (91) liegt dann $\sqrt{\alpha_{n-1}'}$ in A_{n-1}. Dies steht mit (69_2) in einem Widerspruch, womit wir $\Lambda \neq K_n$ bewiesen haben.

Hieraus folgt nach (109_1), daß $\Lambda | K_n$ vom Grad 2 ist. Da ferner α_n als Element von A_n invariant gegenüber U_n ist, so sind die $T_n^k \alpha_n$ $(k = 0, \ldots, 2^n - 1)$ die sämtlichen Konjugierten von α_n (vgl. [32]). Folglich sind die

$$(110) \qquad \pm\sqrt{T_n^k \alpha_n} \qquad (k = 0, \ldots, 2^n - 1)$$

die sämtlichen Konjugierten von $\sqrt{\alpha_n}$, somit ist Λ wegen (94) Galoissch.

Wir zeigen, daß $\Lambda | \Omega$ zyklisch ist. Wegen (110) existiert nämlich ein Automorphismus V von $\Lambda | \Omega$, wofür

$$(111) \qquad V\sqrt{\alpha_n} = \sqrt{T_n \alpha_n}$$

ist. Da $\Lambda | \Omega$ vom Grad 2^{n+1} ist, so genügt es zu zeigen, daß

$$(112) \qquad V^{2^n} \neq 1$$

ist. Wegen (111) gilt $V\alpha_n = T_n \alpha_n$, also

$$(113) \qquad V^{2^{n-1}} \alpha_n = T_n^{2^{n-1}} \alpha_n = \alpha_n',$$

wobei berücksichtigt wurde, daß $T_n^{2^{n-1}}$ der einzige nicht identische Isomorphismus von $A_n | A_{n-1}$ in K_n ist. Folglich läßt sich (91) so schreiben:

$$\alpha_n \cdot V^{2^{n-1}} \alpha_n \underset{(2)}{=} \alpha_{n-1}' \qquad (\text{in } A_{n-1}),$$

also gilt eine Gleichung

$$(114) \qquad \sqrt{\alpha_n} \cdot V^{2^{n-1}} \sqrt{\alpha_n} = \alpha \sqrt{\alpha_{n-1}'} \qquad (\alpha \in A_{n-1}).$$

Wenn nun (112) falsch, d. h. $V^{2^n} = 1$ ist, so bleibt die linke Seite von (114) bei Anwendung von $V^{2^{n-1}}$ invariant. Wegen $\alpha \in K_{n-1}$ gilt ähnliches über α, folglich ist

$$V^{2^{n-1}} \sqrt{\alpha_{n-1}'} = \sqrt{\alpha_{n-1}'}.$$

Da ferner nach (69_2)

$$K_n = K_{n-1}(\sqrt{\alpha_{n-1}'})$$

ist, so folgt, daß $V^{2^{n-1}}$ bei Anwendung auf K_n den identischen Automorphismus induziert. Dies ist wegen (113) ein Widerspruch, womit wir bewiesen haben, daß ((112) richtig also) $\Lambda | \Omega$ zyklisch ist.

Nach (109) ist

$$D_{\Lambda | K_n} | D_{B | A_n}.$$

Die rechte Seite also noch mehr die linke ist wegen (109_2), (92), (93) und $(2, \mathfrak{m}_{n-1}) = 1$ ein Teiler von

$$\mathfrak{d}_n \mathfrak{m}_{n-1}^{2^{-1}}.$$

Da K_n, Λ Galoissch sind, so gilt die ähnliche Teilbarkeit auch für die Kon-

jugierten dieses Ideals, insbesondere also auch für

$$\mathfrak{d}_n' \mathfrak{m}_{n-1}^{2^{-1}}.$$

Hieraus folgt wegen (95_2)

(115) $$D_{\Lambda|K_n} | \mathfrak{m}_{n-1}^{2^{-1}}.$$

Bezeichne $\mathfrak{h}$ und $\mathfrak{f}$ die Λ zugeordnete Idealgruppe in Ω bzw. den endlichen Teil ihres Führers. Zur Berechnung von $\mathfrak{f}$ wenden wir die Formeln (81), (82) mit Λ, K_n statt K_n, K_{n-1} an:

$$D_{\Lambda|\Omega} = \mathfrak{f}_1 \mathfrak{f}_2^2 \cdots \mathfrak{f}_n^{2^{n-1}} \mathfrak{f}^{2^n},$$

$$D_{\Lambda|\Omega} = D_{\Lambda|K_n}^{2^n} D_{K_n|\Omega}^2,$$

Aus diesen folgt wegen (81)

$$\mathfrak{f}^{2^n} = D_{\Lambda|K_n}^{2^n} D_{K_n|\Omega}.$$

Nach (115) gilt dann

$$\mathfrak{f}^{2^n} | \mathfrak{m}_{n-1}^{2^{n-1}} D_{K_n|\Omega}.$$

Die rechte Seite ist nach (81), (83) gleich $\mathfrak{f}_n^{2^n}$. Hiernach gilt

(116) $$\mathfrak{f} | \mathfrak{f}_n.$$

Wegen (84) folgt hieraus zunächst $\mathfrak{f} | \mathfrak{m}$. Wegen der Definition von $\mathfrak{f}$ gilt also $H_{\mathfrak{m}} \subseteq \mathfrak{h}$. Andererseits ist $g(\Lambda|\Omega) = 2^{n+1}$, somit gilt sogar $H \subseteq \mathfrak{h}$. Folglich ist Λ ein K_{n+1}. Für die entsprechende Zahl $\mathfrak{m}_{n+1}$ gilt also wegen (84) $\mathfrak{f} = \mathfrak{f}_n \mathfrak{m}_{n+1}$. Dies mit (116) zusammen ergibt $(\mathfrak{f} = \mathfrak{f}_n)$, $\mathfrak{m}_{n+1} = 1$.

Nach (109_2) ist der Körper B offenbar ein von K_n verschiedener Körper zwischen A_n und $\Lambda = K_{n+1}$, also ein A_{n+1}. Wir haben nur noch zu zeigen, daß diesem $B = A_{n+1}$ eben das Ideal $\mathfrak{d}_n$ zugehört. Zu diesem Zweck bezeichnen wir mit $\mathfrak{d}_n^*$ das A_{n+1} (im Sinne von Satz 5) zugehörige Ideal. Aus (56), (59_3) (angewendet mit $n+1$ statt n) folgt, daß

(117) $$\mathfrak{d}_n^* | D_{A_{n+1}|A_n}$$

ist und (95_1) auch mit $\mathfrak{d}_n^*$ statt $\mathfrak{d}_n$ gilt. Wegen des Bestehens von (95_1) für $\mathfrak{d}_n^*$ und $\mathfrak{d}_n$ sind die Primidealfaktoren dieser Ideale paarweise gleich oder konjugiert. Wenn also $\mathfrak{d}_n^* \neq \mathfrak{d}_n$ wäre, so gibt es ein Primideal $\mathfrak{p}$ in A_n mit

(118) $$\mathfrak{p} | \mathfrak{d}_n$$

und $\mathfrak{p}' | \mathfrak{d}_n^*$, wobei $\mathfrak{p}'$ das Konjugierte von $\mathfrak{p}$ in $A_n | A_{n-1}$ ist. Nach (117) gilt dann

(119) $$\mathfrak{p}' | D_{A_{n+1}|A_n}.$$

Nach (118), (95_2) ist $\mathfrak{p} \nmid \mathfrak{d}_n'$, also

(120) $$\mathfrak{p}' \nmid \mathfrak{d}_n.$$

Da auch ($\mathfrak{p}' \nmid \mathfrak{m}$ also) $\mathfrak{p}' \nmid \mathfrak{m}_{n-1}$ ist, so folgt aus $A_{n+1} = A_n(\sqrt{\alpha_n})$ und aus (92), (119), daß

(121) $$\mathfrak{p}' | 2$$

und

$$\alpha_n \underset{(2)}{\not\equiv} 1 \pmod{\mathfrak{p}'^2} \qquad (\text{in } \mathsf{A}_n)$$

gelten. Andererseits gilt nach (93), (120), (121) eben das Gegenteil. Mit diesem Widerspruch haben wir den Beweis von Satz 6 beendet.

BEWEIS DES ZUSATZES VON SATZ 6. Zur Vorbereitung beweisen wir zwei Hilfssätze..

HILFSSATZ 6. *Wenn $L|K$ ein relativquadratischer Körper ist und eine Gleichung*

(122) $$N_{L|K}\alpha \underset{(2)}{=} N_{L|K}\beta \qquad (\text{in } K) \qquad (\alpha, \beta \in L)$$

gilt, so gilt eine Gleichung

(123) $$\alpha \underset{(2)}{=} \beta\gamma \qquad (\text{in } L) \qquad (\gamma \in K).$$

BEMERKUNG. Da umgekehrt aus (123) trivial (122) folgt, so besagt Hilfssatz 6 kurz, daß (122) nur trivial befriedigt sein kann.

Im Spezialfall $\beta = 1$ folgt die Behauptung sofort aus der Identität

$$u(u+v+2\sqrt{uv}) = (u+\sqrt{uv})^2,$$

wenn man α und sein Konjugiertes in $L|K$ für u bzw. v einsetzt. Der allgemeine Fall folgt aus dem jetzt bewiesenen speziellen, wenn man diesen mit $\alpha\beta^{-1}$ statt α anwendet.

HILFSSATZ 7. *Man nehme an, daß bei einem i $(1 \leqq i \leqq n-1)$ (91), (92), (93), (95), (100) erfüllt sind, daß dasselbe (mit gemeinsamem $\mathfrak{d}_n$) auch für ein $\beta_n (\in \mathsf{A}_n)$ statt α_n gilt, und daß $D'_n \neq 1, -4$ ist. Dann gibt es ein $\omega_i (\in \mathsf{A}_i)$ mit*

$$\left.\begin{aligned} &(124) & \beta_n &\underset{(2)}{=} \alpha_n \omega_i \\ &(125) & (\omega_i) &\underset{(2)}{=} 1 \\ &(126) & \omega_i &\underset{(2)}{\equiv} 1 \pmod 4 \end{aligned}\right\} (\text{in } \mathsf{A}_n).$$

Da man nämlich (91) auch als

$$N_{\mathsf{A}_n|\mathsf{A}_{n-1}}\alpha_n \underset{(2)}{=} \alpha'_{n-1} \quad (\text{in } \mathsf{A}_n)$$

schreiben kann und nach der Annahme die ähnliche Gleichung auch für β_n statt α_n gilt, so hat man

$$N_{\mathsf{A}_n|\mathsf{A}_{n-1}}\alpha_n \underset{(2)}{=} N_{\mathsf{A}_n|\mathsf{A}_{n-1}}\beta_n \quad (\text{in } \mathsf{A}_n).$$

Hieraus folgt nach Hilfssatz 6 zunächst die Existenz einer Zahl $\omega_i (\in \mathsf{A}_{n-1})$, wofür (124) gilt. Da ferner (92), (93) auch für β_n (statt α_n) gelten, so folgt hieraus durch Dividieren das Bestehen von (125) und von

$$\omega_i \underset{(2)}{\equiv} 1 \left(\operatorname{mod} \frac{4}{(2, \mathfrak{d}_n)^2}\right) (\text{in } \mathsf{A}_n).$$

Übergeht man hier auf das Konjugierte in $A_n|A_{n-1}$, so folgt wegen $\omega_i \in A_{n-1}$ das Bestehen einer ähnlichen Kongruenz mit $\mathfrak{d}_n'$ statt $\mathfrak{d}_n$. Aus beiden Kongruenzen folgt wegen (95_2) die Kongruenz (126). Bisher haben wir bewiesen, daß (124) bis (126) mit einem $\omega_i (\in A_{n-1})$ erfüllt sind.

Im Fall $i = n-1$ war das eben die Behauptung. Im übriggebliebenen Fall $i \leq n-2$ nehmen wir die Richtigkeit der Behauptung für $i+1$ statt i an und schließen mit Induktion, wie folgt. Mit (100) zusammen gilt die ähnliche Gleichung für $i+1$ statt i, was man so einsieht, daß man auf (100) den Automorphismus $T_n^{2^i}$ ausübt und beide Gleichungen miteinander multipliziert. Hiernach folgt aus der Induktionsannahme, daß (124) bis (126) mit einem $\omega_i (\in A_{i+1})$ erfüllt sind. Für dieses ω_i folgt wegen (124) aus (100) und der ähnlichen Gleichungen für β_n (statt α_n) durch Dividieren

$$\omega_i \cdot T_n^{2^i} \omega_i \underset{(2)}{=} 1 \quad (\text{in } K_n).$$

Da nach dem Teil 1° von Satz 5 der Unterkörper A_k von K_n zur Untergruppe $\{T_n^{2^k}, U_n\}$ von $\mathfrak{G}(K_n)$ gehört ($k = 0, \ldots, n$), so besagt die letzte Gleichung das Bestehen von

$$N_{A_{i+1}|A_i} \omega_i = \eta^2$$

mit einem η in K_n. Eben wegen dieser Gleichung gilt aber $\eta^2 \in A_i$, somit ist $A_i(\eta)$ ein Unterkörper von K_n höchstens vom zweiten Grade über A_i. Folglich liegt η nach (53) in einem der Körper A_{i+1}, K_i, A_{i+1}, also gilt nach (68_2), (51), bzw. (63)

(127) $$N_{A_{i+1}|A_i} \omega_i = (\alpha + \beta \sqrt{\gamma})^2$$

mit passenden $\alpha, \beta (\in A_i)$ und $\gamma = \alpha_i', D$ oder α_i.

Wenn $\beta = 0$ ist, so folgt aus (127) und Hilfssatz 6

$$\omega_i \underset{(2)}{=} \omega_i^* \qquad (\text{in } A_{i+1})$$

mit einem $\omega_i^* (\in A_i)$. Da dann noch mehr $\omega_i \underset{(2)}{=} \omega_i^*$ (in A_n) gilt, so sind jetzt (124) bis (126) auch für ω_i^* statt ω_i erfüllt, somit ist Hilfssatz 7 in diesem Fall richtig.

Wenn $\beta \neq 0$ ist, so muß $\alpha = 0$ sein, denn sonst würde aus (127) $\sqrt{\gamma} \in A_i$ folgen, was aber in allen drei Fällen falsch ist. Hiernach folgt jetzt aus (127)

(128) $$N_{A_{i+1}|A_i} \omega_i \underset{(2)}{=} \gamma \quad (\text{in } A_i).$$

Erstens sei $\gamma = \alpha_i'$. Wir setzen

$$\omega_i^* = \alpha_{i+1} \omega_i .$$

Dieses ω_i^* liegt ebenfalls in A_{i+1}, ferner gilt nach (64_3), (128)

$$N_{A_{i+1}|A_i} \omega_i^* \underset{(2)}{=} \alpha_i'^2 \underset{(2)}{=} 1 \quad (\text{in } A_i).$$

Hieraus folgt nach Hilfssatz 6

$$\omega_i^* \underset{(2)}{=} \omega_i^{**} \text{ (in } A_{i+1})$$

mit einem ω_i^{**} in A_i. Wegen $i \leqq n-2$ ist $\alpha_{i+1} \underset{(2)}{=} 1$ (in A_n), somit haben wir

$$\omega_i \underset{(2)}{=} \omega_i^{**} \text{ (in } A_n).$$

Hiernach sind wir zu ähnlichem Schluß gekommen wie oben im Fall $\beta = 0$, weshalb Hilfssatz 7 auch jetzt richtig ist.

Zweitens sei $\gamma = D$. Wir werden zeigen, daß dieser Fall widersprüchig ist. Schreiben wir (128) in der Form

(129) $$D \cdot N_{A_{i+1}|A_i} \omega_i \underset{(2)}{=} 1 \text{ (in } A_i).$$

Wir setzen

(130) $$(\omega_i) \underset{(2)}{=} \mathfrak{b}_{i+1} \text{ (in } A_{i+1})$$

mit einem quudratfreien ganzen Ideal $\mathfrak{b}_{i+1}$ in A_{i+1}. Dann gilt nach (129), (130)

(131) $$D \cdot N_{A_{i+1}|A_i} \mathfrak{b}_{i+1} \underset{(2)}{=} 1 \text{ (in } A_i).$$

Nach (125), (130) ist $\mathfrak{b}_{i+1}$ ein Idealquadrat in A_{i+1}. Dann gilt für das Ideal

(132) $$\mathfrak{c}_{i+1} = (D, \mathfrak{b}_{i+1})$$

in A_{i+1} ebenfalls

(133) $$\mathfrak{c}_{i+1} \underset{(2)}{=} 1 \text{ (in } A_n).$$

Aus (131), (132) folgt

(134) $$D \cdot N_{A_{i+1}|A_i} \mathfrak{c}_{i+1} \underset{(2)}{=} 1 \text{ (in } A_i).$$

Man berücksichtige, daß nach der dem Satz 5 angefügten Bemerkung unter allen Primidealfaktoren von D in A_{i+1} nur die Teiler von $\mathfrak{d}_{i+1}$ Idealquadrate in A_n sind. Hieraus und aus (132), (133) folgt $\mathfrak{c}_{i+1} | \mathfrak{d}_{i+1}$, also nach (59_3)

(135) $$N_{A_{i+1}|A_i} \mathfrak{c}_{i+1} | \mathfrak{d}_i'.$$

Nun folgt aus (56), daß $\mathfrak{d}_0, \ldots, \mathfrak{d}_{i-1}$ Idealquadrate in A_i sind, somit gilt nach (61)

$$\mathfrak{d}_i \mathfrak{d}_i' \underset{(2)}{=} D \text{ (in } A_i).$$

Dies ergibt nach (134)

$$N_{A_{i+1}|A_i} \mathfrak{c}_{i+1} \underset{(2)}{=} \mathfrak{d}_i \mathfrak{d}_i' \text{ (in } A_i).$$

Wegen (60) folgt hieraus nach (135)

$$\mathfrak{d}_i \underset{(2)}{=} 1 \text{ (in } A_i).$$

Man bilde die Norm in A_i. Es folgt nach (62)

$$(D_0') \underset{(2)}{=} 1 \text{ (in } P).$$

Dies ergibt, daß D_0' entweder 1 oder -4 ist. Eben diese Fälle haben wir aber ausgeschlossen, weshalb der jetzt betrachtete Fall $\gamma = D$ unmöglich ist.

Drittens sei $\gamma = \alpha_i$. Wir zeigen, daß auch dieser Fall unmöglich ist, so daß wir ihn auf den vorigen Fall zurückführen. Da $\alpha_0, \ldots, \alpha_{i-1}$ Quadratzahlen in A_i sind, so folgt aus (64) leicht, daß

$$\alpha_i \underset{(2)}{=} \alpha_i' D \text{ (in } \mathrm{A}_i)$$

ist. Folglich ist jetzt nach (128)

$$N_{\mathrm{A}_{i+1} \mid \mathrm{A}_i} \omega_i \underset{(2)}{=} \alpha_i' D \text{ (in } \mathrm{A}_i).$$

Wir führen die Zahl

$$\omega_i^* = \alpha_{i+1}\, \omega_i$$

ein, die ebenfalls in A_{i+1} liegt (wie auch ω_i). Da α_{i+1} wegen $i \leqq n-2$ ein Quadrat in A_n ist, so gelten (124) bis (126) auch für ω_i^* statt ω_i. Ferner gilt wegen (64_3)

$$N_{\mathrm{A}_{i+1} \mid \mathrm{A}_i} \omega_i^* \underset{(2)}{=} \alpha_{i+1} \alpha_{i+1}' \alpha_i' D \underset{(2)}{=} \alpha_i'^2 D \underset{(2)}{=} D \text{ (in } \mathrm{A}_i).$$

Der Vergleich mit (128) zeigt, daß dieser Fall in der Tat auf den vorigen zurückgeführt wurde. Wir haben den Beweis von Hilfssatz 7 beendet.

Nach diesen Vorbereitungen fangen wir es nunmehr mit dem eigentlichen Beweis des Zusatzes von Satz 6 an. Vor allem wollen wir zeigen, daß aus der Lösbarkeit von (91) die von (97) folgt. Hierzu nehmen wir eine Lösung von (91) in der Form

$$\alpha_n = \alpha + \beta \sqrt{\alpha_{n-1}} \qquad (\alpha, \beta \in \mathrm{A}_{n-1})$$

an. Dann gilt nach (91) eine Gleichung $\alpha^2 - \alpha_{n-1}\beta^2 = \alpha_{n-1}'\gamma^2$, d. h.

$$\alpha^2 = \alpha_{n-1}\beta^2 + \alpha_{n-1}'\gamma^2 \qquad (\gamma \in \mathrm{A}_{n-1},\ \neq 0). \tag{136}$$

Wegen (96) ist

$$2x = \alpha_{n-1} + \alpha_{n-1}'. \tag{137}$$

Aus beiden folgt

$$2x\alpha^2 = (\alpha_{n-1}\beta + \alpha_{n-1}'\gamma)^2 + \alpha_{n-1}\alpha_{n-1}'(\beta - \gamma)^2,$$

also nach (98)

$$2x\alpha^2\zeta^2 = (\alpha_{n-1}\beta + \alpha_{n-1}'\gamma)^2\zeta^2 + D_0' m_1 (\beta - \gamma)^2. \tag{138}$$

Es kann nicht $\alpha = 0$ sein, denn dann würde nach (136)

$$\alpha_{n-1}\alpha_{n-1}' \underset{(2)}{=} -1 \text{ (in } \mathrm{A}_{n-1})$$

sein. Hieraus folgt nach (64)

$$D_0' m_1 \underset{(2)}{=} -1 \text{ (in } \mathrm{A}_{n-1}),$$

also

$$D_0 m_1 \underset{(2)}{=} -D \text{ (in } \mathrm{A}_{n-1}).$$

Dies bedeutet nach (55_1), daß $\mathrm{P}(\sqrt{-D})$ in A_{n-1} enthalten, also gleich A_1 ist. Folglich gilt die letzte Gleichung auch in P. Dann ist

$$D_0' \underset{(2)}{=} -m_1 \text{ (in P)}$$

also ($m_1 = 1$ und) $D_0' = -4$. Diesen Fall haben wir aber ausgeschlossen, somit ist in der Tat $\alpha \neq 0$. Wegen (98) ist auch $\zeta \neq 0$. Hiernach und nach (138) ist also (97) lösbar, was wir zeigen wollten.

Jetzt zeigen wir, daß (99) für jede Lösung ϱ, σ, τ von (97) eine Lösung α_n von (91) liefert. Aus (99) folgt

$$\alpha_n \alpha_n' = 4x^2\tau^2 - \alpha_{n-1}(\varrho + \alpha_{n-1}' \sigma\zeta)^2.$$

Dies ergibt nach (98)

$$\alpha_n \alpha_n' \alpha_{n-1}' \zeta^2 = 4\alpha_{n-1}' x^2 \tau^2 \zeta^2 - D_0' m_1 (\varrho + \alpha_{n-1}' \sigma\zeta)^2.$$

Für das erste Glied der rechten Seite schreibt sich zuerst nach (97), (137)

$$\alpha_{n-1}'(\alpha_{n-1} + \alpha_{n-1}')(\varrho^2 + D_0' m_1 \sigma^2)\zeta^2,$$

dann nach (98)

$$(D_0' m_1 + \alpha_{n-1}'^2 \zeta^2)(\varrho^2 + D_0' m_1 \sigma^2).$$

Also gilt

$$\alpha_n \alpha_n' \alpha_{n-1}' \zeta^2 = (\alpha_{n-1}' \varrho\zeta - D_0' m_1 \sigma)^2.$$

Dies bedeutet wegen $\zeta \neq 0$ das Bestehen von (91). Zusammengefaßt haben wir bisher bewiesen, daß man unter Annahme der Lösbarkeit von (91) eine Lösung auf dem in I beschriebenen Wege gewinnt.

Wir nehmen jetzt an, daß wir eine Lösung $\alpha_n (\in \mathsf{A}_n)$ von (91) schon gefunden haben. Ist dann $\beta_n (\in \mathsf{A}_n)$ eine weitere Lösung von (91), so gilt

$$\alpha_n \alpha_n' \underset{(2)}{=} \beta_n \beta_n' \quad (\text{in } \mathsf{A}_{n-1}),$$

wobei β_n' das Konjugierte von β_n in $\mathsf{A}_n | \mathsf{A}_{n-1}$ ist. Hieraus folgt nach Hilfssatz 6 eine Gleichung

$$\beta_n \underset{(2)}{=} \alpha_n \gamma \quad (\text{in } \mathsf{A}_n) \qquad (\gamma \in \mathsf{A}_{n-1}).$$

Wenden wir dies insbesondere mit einer Lösung β_n von (91), (92), (93), (95) an, so haben wir das Resultat, daß man auf dem in I und II beschriebenen Wege eine Lösung von (91), (92), (93), (95) gewinnt.

Zum Beweis der übrigen Behauptungen des Zusatzas gehen wir von einer Lösung $\alpha_n (\in \mathsf{A}_n)$ von (91), (92), (93), (95) und (100) aus. Zunächst haben wir die Existenz eines $\omega_i (\in \mathsf{A}_i)$ mit (105) bis (107) auszuweisen. Zu diesem Zweck betrachten wir nach Satz 6 eine Lösung $\beta_n (\in \mathsf{A}_n)$ von (91) bis (95). Dabei dürfen wir nach der zweiten Hälfte der Anmerkung [39] annehmen, daß α_n und β_n die Bedingungen (92), (93) mit *gemeinsamem* $\mathfrak{d}_n$ erfüllen. Da (100) aus (94) folgt, so genügen α_n, β_n den Bedingungen in Hilfssatz 7. Hiernach gibt es ein $\omega_i (\in \mathsf{A}_i)$, wofür (124) bis (126) gelten. Da man β_n mit einem Quadratfaktor in A_n multiplizieren darf, so darf statt (124) sogar

(139) $$\beta_n = \alpha_n \omega_i$$

angenommen werden. Bequemlichkeitshalber schreiben wir (125), (126) noch-

mal hin:

$$\left.\begin{array}{ll}(140) & (\omega_i) \underset{(2)}{\equiv} 1 \\ (141) & \omega_i \underset{(2)}{\equiv} 1 \pmod 4\end{array}\right\} \text{(in } A_n).$$

Da ferner (94) für β_n gilt, so gilt noch mehr

(142) $$\beta_n \cdot T^{2^{i-1}} \beta_n \underset{(2)}{\equiv} 1 \quad (\text{in } K_n).$$

Da β_n eine Lösung von (91) bis (95) ist, so folgt aus Satz 6, daß $K_n(\sqrt{\beta_n})$ ein K_{n+1} und $A_n(\sqrt{\beta_n})$ ein in diesem enthaltenes A_{n+1} ist. Wir können also Satz 5 auf dieses Körperpaar K_{n+1}, A_{n+1} anwenden. Entsprechend können wir nach (49), (54)

$$\mathfrak{G}(K_{n+1}) = \{T, U\}, \quad \mathfrak{G}(K_n | \Omega) = \{T\}$$

setzen mit der Vereinbarung, daß A_{n+1} zur Untergruppe $\{U\}$ gehört. Hiernach sind die Automorphismen T, U je eine Fortsetzung von T_n, U_n, weshalb T, U bei Anwendung auf K_n durch T_n, U_n ersetzt werden dürfen.

Es gelten

(143) $$T\sqrt{D} = \sqrt{D}, \quad T^{2^n}\sqrt{\beta_n} = -\sqrt{\beta_n},$$

(144) $$U\sqrt{D} = -\sqrt{D}, \quad U\sqrt{\beta_n} = \sqrt{\beta_n},$$

(145) $$T^{2^{n+1}} = 1, \quad U^2 = 1, \quad UTU^{-1} = T^{-1}$$

Wir setzen

(146) $$\gamma = \sqrt{\beta_n} \cdot T^{2^{i-1}} \sqrt{\beta_n},$$

(147) $$\gamma_a = T^{a 2^{i-1}} \gamma \qquad (a = 0, \pm 1, \ldots).$$

Wegen (142) gehören γ, also auch alle γ_a in K_n. Wir zeigen für alle a die Formeln:

(148) $$\gamma_a = \gamma_{a+2j} \qquad (j = 2^{n-1}),$$

(149) $$T^{2^{i-1}} \gamma_a = \gamma_{a+1},$$

(150) $$U \gamma_a = \gamma_{-a-1}.$$

Hiervon ist (149) eine Folgerung aus (147). Nach (147), (146), (143_2) ist

$$\gamma_{2j} = T^{2^n} \gamma = \gamma.$$

Hieraus und aus (147) folgt (148). Endlich gilt nach (147), (146)

$$U\gamma_a = UT^{a2^{i-1}} \gamma = UT^{a2^{i-1}} \sqrt{\beta_n} \cdot UT^{(a+1)2^{i-1}} \sqrt{\beta_n},$$

also nach (145), (144_2)

$$U\gamma_a = T^{-a2^{i-1}} \sqrt{\beta_n} \cdot T^{-(a+1)2^{i-1}} \sqrt{\beta_n} = T^{-(a+1)2^{i-1}} (\sqrt{\beta_n} \cdot T^{2^{i-1}} \sqrt{\beta_n}).$$

Die rechte Seite ist nach (146), (147) gleich γ_{-a-1}, womit wir auch (150) bewiesen haben.

Man setze

(151) $$\delta_1 = \gamma_0 + \gamma_2 + \cdots + \gamma_{2j-2}, \quad \delta_2 = \gamma_1 + \gamma_3 + \cdots + \gamma_{2j-1},$$

(152) $$\delta = \delta_1 + \delta_2.$$

Nach (148) bis (150) gelten

$$T^{2^{i-1}}\delta_1 = \delta, \quad T^{2^{i-1}}\delta_2 = \delta_1,$$
$$U\delta_1 = \delta_2, \quad U\delta_2 = \delta_1.$$

Da hiernach δ invariant gegenüber $\{T^{2^{i-1}}, U\}$ ist, so folgt

(153) $$\delta \in \mathsf{A}_{i-1}.$$

Da $\mathfrak{G}(\mathsf{K}_n|\mathsf{K}_{i-1}) = \{T_n^{2^{i-1}}\}$ ist, so folgt aus (152), (151), (148), (149) leicht

(154) $$\delta^2 = S_{\mathsf{K}_n|\mathsf{K}_{i-1}}[\gamma_0(\gamma_0 + 2\gamma_1 + \cdots + 2\gamma_{j-1} + \gamma_j)].$$

Wir setzen noch

(155) $$\mu_a^* = \gamma_0\gamma_a \qquad (a = 0, \pm 1, \ldots).$$

Dann gilt nach (147), (146)

$$\mu_0^* = \gamma_0^2 = \gamma^2 = \beta_n \cdot T^{2^{i-1}}\beta_n.$$

Hieraus folgt nach (139), (103_1)

(156) $$\mu_0^* = \omega_i\omega_i'\mu_0,$$

wobei ω_i' das Konjugierte von ω_i in $\mathsf{A}_{i+1}|\mathsf{A}_i$ ist.

Ferner folgt aus (155), (147)

$$\frac{\mu_a^*}{\mu_{a-1}^*} = \frac{\gamma_a}{\gamma_{a-1}} = T^{a2^{i-1}}\gamma \cdot T^{(a-1)2^{i-1}}\gamma^{-1} = T^{(a-1)2^{i-1}}(\gamma^{-1} \cdot T^{2^{i-1}}\gamma).$$

Das Produkt auf der rechten Seite ist wegen (146) gleich

$$(\sqrt{\beta_n})^{-1}\, T^{2^i}\sqrt{\beta_n}.$$

Hierfür schreibt sich wegen (139) und $T^{2^i}\omega_i = \omega_i$ vom Vorzeichen abgesehen zuerst

$$(\sqrt{\alpha_n})^{-1}\, T^{2^i}\sqrt{\alpha_n},$$

dann nach (101) einfach $\alpha_n^{-1}\mu$. Wird also das Vorzeichen von μ in (101) passend gewählt, was uns ja frei steht, so gilt

(157) $$\mu_a^* = \mu_{a-1}^* \cdot T^{(a-1)2^{i-1}}(\alpha_n^{-1}\mu) \qquad (a = 0, \pm 1, \ldots).$$

Wegen (103_2) folgt hieraus zunächst

$$\mu_a^{-1}\mu_a^* = \mu_{a-1}^{-1}\mu_{a-1}^* \qquad (a = 1, \ldots, j),$$

also

$$\mu_a^{-1}\mu_a^* = \mu_0^{-1}\mu_0^* \qquad (a = 0, \ldots, j),$$

dann nach (156)

(158) $$\mu_a^* = \omega_i\omega_i'\mu_a \qquad (a = 0, \ldots, j).$$

Aus (154), (155), (158) bekommen wir

$$\delta^2 = \omega_i \omega_i' S_{K_n|K_{i-1}}(\mu_0 + 2\mu_1 + \cdots + 2\mu_{j-1} + \mu_j),$$

also nach (104)

$$\delta^2 \doteq \omega_i \omega_i' \omega. \tag{159}$$

Nunmehr können wir zunächst (108) beweisen. Da nach (147) $\gamma_0 = \gamma$ ist, so folgt aus (159)

$$\gamma^2 \omega_i \omega_i' \omega = (\gamma_0 \delta)^2.$$

Die linke Seite ist wegen (146), (139) und $T^{2^{i-1}} \omega_i = \omega_i'$ gleich

$$(\omega_i \omega_i')^2 \alpha_n \cdot T^{2^{i-1}} \alpha_n \cdot \omega.$$

Die rechte Seite ist wegen (152), (151), (155) gleich

$$(\mu_0^* + \cdots + \mu_{2j-1}^*)^2.$$

Wenn nun die Definition (103) auf alle $a = 0, \pm 1, \ldots$ erstreckt wird, so bleibt (158) (mit unverändertem Beweis) richtig. Somit geht der vorige Ausdruck in

$$(\omega_i \omega_i')^2 (\mu_0 + \cdots + \mu_{2j-1})^2$$

über. Hieraus folgt die Richtigkeit von (108).

Wegen (153), (159) gilt

$$\omega_i \omega_i' \underset{(2)}{=} \omega \qquad (\text{in } A_n).$$

Dies mit (140), (141) zusammen beweist die Lösbarkeit von (105) bis (107).

Um die Schlußbehauptung in Teil III des Zusatzes zu beweisen, setzen wir

$$\alpha_n^* = \omega_i \alpha_n,$$

wobei jetzt $\omega_i (\in A_i)$ eine beliebige Lösung von (105) bis (107) bezeichnen soll. Aus (105), (108) folgt durch Multiplikation wegen $\omega_i' = T^{2^{i-1}} \omega_i$:

$$\omega_i \alpha_n \cdot T^{2^{i-1}} (\omega_i \alpha_n) \underset{(2)}{=} (\mu_0 + \cdots + \mu_{2j-1})^2 \qquad (\text{in } A_n).$$

Folglich gilt

$$\alpha_n^* \cdot T^{2^{i-1}} \alpha_n^* \underset{(2)}{=} 1 \qquad (\text{in } K_n).$$

Dies bedeutet, daß $\alpha_n^* (\in A_n)$ der Bedingung (100) mit $i-1$ statt i genügt. Da α_n^* wegen (106), (107) mit α_n zusammen auch den Bedingungen (91), (92), (93), (95) genügt, so haben wir die gesagte Behauptung bewiesen, und auch den Beweis des Zusatzes beendet.

§ 7. Einige Teilresultate und Beispiele

Unsere Sätze 1 bis 6 nebst dem Zusatz von Satz 6 liefern auf Grund der Arbeit [8] die vollständige Beantwortung unserer Probleme I bis IV. Wie schon mehrmals gesagt, geschieht diese Beantwortung so, daß man nach und nach die Matrizen $M_1, M_2, \ldots$ (vgl. [8], (15)) mit Hilfe des in [8], § 3 be-

schriebenen Algorithmus aufstellt. (Für die konstruktive Ausführung s. man [8] § 6.) Wir wollen hier sehen, wie der Anfang dieses Algorithmus aussieht, wodurch wir auch einige explizite Sätze bekommen werden. Auch arbeiten wir dann ein einfaches numerisches Beispiel aus.

Als wichtige Vorbereitung wollen wir sehen, wie ein beliebiges bedingtes Artinsches Symbol

$$\left(\frac{K}{A}\right)_n \tag{160}$$

berechnet werden kann ($1 \leqq n \leqq \nu$), wobei wir seine Existenz selbstverständlich voraussetzen. Dabei setzen wir nach Satz 5

$$K = K_1 = \Omega(\sqrt{D_0 m_1}), \tag{161}$$

ferner nehmen wir A nach Satz 1 in der Form

$$A = A(\mathfrak{S}), \qquad \mathfrak{S} = (d', d'', m', m'') \tag{162}$$

an. Außerdem nehmen wir eine Zahl

$$\xi = m'x'\sqrt{d'} + m''x''\sqrt{d''} \tag{163}$$

mit den in (19) bis (21) beschriebenen Eigenschaften zu Hilfe. Dann ist A eben diejenige Idealklasse, die das Ideal (ξ) in Ω enthält. Aus dem Satz der arithmetischen Progression folgt leicht, daß (ξ) auch als ein zu 2 primes Primideal in Ω angenommen werden kann. Das bedeutet, daß

$$d'm'^2x'^2 - d''m''^2x''^2 = r \tag{164}$$

eine zu $2m$ prime positive Primzahl ist.

Um nun (160) zu berechnen, nehmen wir ein K_n über K zu Hilfe, wofür wir auch die Bezeichnungen im Satz 5 übernehmen. Mit diesen Bezeichnungen gilt

$$K_n = K_{n-1}(\sqrt{\alpha_n}). \tag{165}$$

Da in Ω die Primidealzerlegung $r = (\xi)(\xi')$ gilt, wobei ξ' das Konjugierte von ξ in $\Omega(\sqrt{d})|P(\sqrt{d})$ bezeichnet, so ist (ξ) ein Primideal ersten Grades in $A(\mathfrak{S})$. Wegen der Existenz von (160) und der Definition in [8] § 2 zerfällt (ξ) in $K_{n-1}|\Omega$ voll, also zerfällt r in K_{n-1} ebenfalls voll. Bezeichne $\mathfrak{R}$ einen beliebigen Primidealfaktor von r in K_{n-1}. Dann folgt aus (165) offenbar

$$\left(\frac{K}{A(\mathfrak{S})}\right)_n = \left(\frac{\alpha_{n-1}|K_{n-1}}{\mathfrak{R}}\right), \tag{166}$$

wobei rechts das übliche Zeichen für das zweite Potenzrestsymbol steht. Da $\mathfrak{R}$ vom ersten Grade ist, so gilt

$$\alpha_{n-1} \underset{(2)}{\equiv} c_{n-1} \pmod{\mathfrak{R}} \qquad (\text{in } K_{n-1})$$

mit einer (zu $\mathfrak{R}$ also auch) zu r primen ganzen rationalen Zahl c_{n-1}, die sich natürlich leicht bestimmen läßt. Dann folgt aus (166)

$$\left(\frac{K}{A(\mathfrak{S})}\right)_n = \left(\frac{c_{n-1}|P}{r}\right) = \left(\frac{c_{n-1}}{r}\right). \tag{167}$$

Hiernach macht die Berechnung der bedingten Artinschen Symbole keine Schwierigkeiten.

Nunmehr setzen wir

$$m = p_1 \cdots p_s, \tag{168}$$

$$D = d_{s+1} \cdots d_t, \tag{169}$$

wobei $p_1, \ldots, p_s$ (verschiedene) primäre Primzahlen und $d_{s+1}, \ldots, d_t$ die Stammdiskriminantenfaktoren von D sind. Wir wählen die Bezeichnungen so, daß im Fall $2|D$ eben $2|d_t$ ist. Ferner bezeichnen wir mit p_i $(i = s+1, \ldots, t)$ den (einzigen) Primzahlfaktor von d_i. Und zwar wenn $2 \nmid d_i$ ist, so darf einfach $p_i = d_i$ gesetzt werden, wenn dagegen $2|d_t$ ist, so soll $p_t = 2$ sein. Endlich setzen wir

$$q_i = |p_i|. \tag{170}$$

Nach Satz 1 bilden die Körper

$$K^{(k)} = \Omega(\sqrt{p_k}) \qquad (k = 1, \ldots, t-1) \tag{171}$$

und die Systeme

$$\mathfrak{S}^{(i)} = \left(1, d, p_i, \frac{m}{p_i}\right) \qquad (i = 1, \ldots, s), \tag{172}$$

$$\mathfrak{S}^{(i)} = \left(q_i, \frac{d}{q_i}, 1, m\right) \qquad (i = s+1, \ldots, t) \tag{173}$$

eine Basis der Körpermenge $\mathfrak{M}_1$ bzw. der Gruppe $\mathfrak{S}$.[44] Diese Basen wollen wir bei der Aufstellung der Matrix M_1 zugrunde legen.

Das Element in der i-ten Zeile und k-ten Spalte von M_1 ist dann

$$\left(\frac{K^{(k)}}{A(\mathfrak{S}^{(i)})}\right)_1 \quad (i = 1, \ldots, t;\ k = 1, \ldots, t-1). \tag{174}$$

Um dies zu berechnen, sei zuerst $i \leqq s$. Für diesen Fall lautet (164) wegen (172) so:

$$p_i^2 x^2 - d\frac{m^2}{p_i^2} y^2 = r. \tag{175}$$

Nach (167), (171) hat dann (174) den Wert

$$\left(\frac{p_k}{r}\right).$$

[44] Wir fassen die Definition der Systeme $\mathfrak{S} = (d', d'', m', m'')$ etwas allgemeiner so, daß wir in den Variabeln d', d'', m', m'' einen von 0 verschiedenen rationalen Quadratzahlfaktor unberücksichtigt lassen. Erst nach dieser Vereinbarung wird (172), (173) auch im Fall $d \equiv 3 \pmod 4$ wirklich eine Basis von $\mathfrak{S}$ bilden, da dann

$$\mathfrak{S}^{(t)} = \left(2, \frac{d}{2}, 1, m\right) = \left(\frac{1}{2}, \frac{d}{2}, 1, m\right)$$

ist.

Hierfür läßt sich nach dem quadratischen Reziprozitätssatz $\left(\frac{r}{p_k}\right)$ schreiben. Dieses Symbol ist nach (175) gleich 1 oder $\left(\left(\frac{-d}{p_k}\right)=\right)\left(\frac{-D}{p_k}\right)$, je nachdem $i \neq k$ oder $i=k$ ist. Im Fall $i \geqq s+1$ werde zunächst $2 \nmid d_i$ angenommen. Dann kann man nach (163), (173) einfach $\xi=\sqrt{q_i}$, $r=q_i$ setzen. Wenn also $i \neq k$ ist, so hat (174) nach (171) einfach den Wert $\left(\left(\frac{p_k}{q_i}\right)=\right)\left(\frac{p_k}{p_i}\right)$. Wenn aber $i=k$ ist, so ergibt sich für (174) nach Berücksichtigung von

$$p_i \underset{(2)}{\equiv} \frac{D}{p_i} \quad (\text{in } \Omega)$$

der Wert $\left(\frac{p_i^{-1} D}{p_i}\right)$. Der übriggebliebene Fall $2 \mid d_i$, d. h. $i=t$, $p_t=2$ macht auch keine Ausnahme. Wenn nämlich $2 \mid d$ ist, so läßt sich

$$2x^2-\frac{d}{2} m^2 y^2=r$$

annehmen, und dann hat (174) den Wert

$$\left(\frac{p_k}{r}\right)=\left(\frac{r}{p_k}\right)=\left(\frac{2}{p_k}\right)=\left(\frac{p_k}{2}\right)=\left(\frac{p_k}{p_t}\right),$$

wobei $\left(\frac{p_k}{2}\right)$ das Kroneckersche Symbol ist. Wenn $d \equiv 3 \pmod 4$ ist, so läßt sich

$$\frac{1}{2} x^2-\frac{d}{2} m^2 y^2=r$$

annehmen, somit kommt man zu ähnlichem Schluß wie vorher.

Wir haben bekommen:

$$M_1=\left|\begin{array}{cccccc}
\left(\frac{-D}{p_1}\right) & \cdots & 1 & 1 & \cdots & 1 \\
\vdots & & & & & \\
1 & & \left(\frac{-D}{p_s}\right) & 1 & & 1 \\
\left(\frac{p_1}{p_{s+1}}\right) & & \left(\frac{p_s}{p_{s+1}}\right) & \left(\frac{p_{s+1}^{-1} D}{p_{s+1}}\right) & & \left(\frac{p_{t-1}}{p_{z+1}}\right) \\
\vdots & & & & & \\
\left(\frac{p_1}{p_{t-1}}\right) & & \left(\frac{p_s}{p_{t-1}}\right) & \left(\frac{p_{s+1}}{p_{t-1}}\right) & & \left(\frac{p_{t-1}^{-1} D}{p_{t-1}}\right) \\
\left(\frac{p_1}{p_t}\right) & & \left(\frac{p_s}{p_t}\right) & \left(\frac{p_{s+1}}{p_t}\right) & & \left(\frac{p_{t-1}}{p_t}\right)
\end{array}\right| \tag{176}$$

Diese Matrix gibt also nach den Sätzen 1 bis 4 folgende Auskunft bezüglich unserer Probleme I bis IV. Reduziere man M_1 nach den Zeilen,[45] wodurch sie die Form

$$\left(\left(\frac{K^{(k)}}{A(\mathfrak{T}^{(i)})}\right)_1\right) \quad (i=1,\ldots,t;\ k=1,\ldots,t-1) \tag{177}$$

erhält mit einer neuen Basis $\mathfrak{T}^{(1)},\ldots,\mathfrak{T}^{(t)}$ von $\mathfrak{T}$. Dann wird die Anzahl e_2 der durch 4 teilbaren Invarianten der Klassengruppe $\mathfrak{H}$ um 1 weniger als die der Zeilen mit lauter Elementen 1 (das sind die ersten e_2 Zeilen und die letzte Zeile). Die zugehörigen e_2+1 Systeme $\mathfrak{S}(=\mathfrak{T}^{(1)},\ldots,\mathfrak{T}^{(e_2)},\mathfrak{T}^{(t)})$ bilden eine Basis der Gruppe $\mathfrak{T}_1$, wodurch also bekannt wird, welche 2^{e_2+1} Gleichungen (2) für $n=2$ lösbar sind. (Fällt insbesondere $e_2=0$ aus, so weiß man auch, für welches $\mathfrak{S}(\neq\mathfrak{S}_1)$ die Dirichletsche Gleichung (3) lösbar, und also ob eben die Pellsche Gleichung (4) lösbar ist.) Reduziert man ferner M_1 („vollständig") aus, so wird auch noch die Menge $\mathfrak{M}_2$ derjenigen $2^{e_2}-1$ Körper K_1 kenntlich, über denen mindestens ein K_2 existiert. Und zwar, wenn man M_1 nach dem Ausreduzieren wieder in der Form (177) annimmt, so bilden die $K^{(1)},\ldots,K^{(e_2)}$ (d. h. die Zähler in den Spalten mit lauter Elementen 1) eben eine Basis von $\mathfrak{M}_2$. (Diese Sätze finden sich für den „absoluten Fall" $m=1$ in den Arbeiten [9], [10], [18]. Vgl. noch [11], [12], ferner [14], wo bezüglich der Pellschen Gleichung (4) auch der Fall eines beliebigen m betrachtet wird.)

Gleich wollen wir aus diesen Resultaten einen wichtigen Schluß ziehen. Insbesondere sollen jetzt alle Faktoren in (168), (169) positiv sein. (Das bedeutet, daß dm^2 eine kritische Zahl ist.) Man liest von (176) ab, das jetzt das Produkt aller Zeilen von M_1 aus lauter Elementen 1 besteht. Dies bedeutet wegen $\mathfrak{S}_1^*=(d,1,m,1)$:

$$\left(\frac{K^{(k)}}{A(\mathfrak{S}_1)}\right)_1=1 \qquad (k=1,\ldots,t-1)$$

also allgemeiner

$$\left(\frac{K}{A(\mathfrak{S}_1)}\right)_1=1 \qquad (K\in\mathfrak{M}_1).$$

Dies besagt nun nach dem Kriterium (36), daß jetzt $\mathfrak{S}_1^*\in\mathfrak{S}_1$ gilt. Da im Fall $e_2=0$ (d. h. $\nu=1$) $\mathfrak{S}_1=\mathfrak{S}_\nu$ ist, so folgt hieraus nach Satz 4 der folgende:[46]

[45] Die Reduktion von M_1 geschieht nach [8] § 3, wobei man sich (statt [8] Sätze 1, 2) der multiplikativen Eigenschaften des Legendre—Jacobi—Kroneckerschen Symbols $\left(\frac{a}{b}\right)$ bedient. Es ist oft nützlich die Multiplikation von Zeilen oder Spalten einer Matrix, deren Elemente einer Abelschen Gruppe zugehören, der üblichen Addition der Zeilen bzw. Spalten einer Matrix ähnlich zu definieren. Kurz gesagt geschieht dann die Reduktion von M_1 durch Zeilen- und Spaltenpermutation und Multiplikation einer Zeile oder Spalte mit einer anderen.

[46] Diesen Satz habe ich — wie schon erwähnt — für den Spezialfall $m=1$ in der Arbeit [9] gefunden. Obige Verallgemeinerung ist neu.

SATZ 7. *Man betrachte solche $d(>0)$, m, die keine positiven Primzahlfaktoren von der Form $4k+3$ haben. Ist $e_2 = 0$, so ist die Pellsche Gleichung* (4) *lösbar.*

BEMERKUNG. Um also diesen Satz anzuwenden, hat man nur die Matrix (176) auszureduzieren. Kommt man dann zu einer Matrix

$$\begin{pmatrix} -1 & & \\ & \ddots & \\ & & -1 \\ 1 & & 1 \end{pmatrix}$$

(in der Diagonale lauter -1, außerhalb der Diagonale lauter 1),[47] so ist (4) lösbar. — Schon dieser elegante Satz 7 allein überzeugt uns von der Wichtigkeit unserer Untersuchungen, da ja umgekehrt Satz 4 als die natürliche Fortsetzung von Satz 7 anzusehen ist.

Jetzt wollen wir sehen, wie sich unser Algorithmus weiter gestaltet, aber einfachheitshalber beschränken wir uns auf den Fall $m=1$ $(s=0)$, $2 \nmid D$. Wir nehmen an, daß wir M_1 schon ausreduziert, und nachher die Ableitung

(178) $$M_2 = \left(\left(\frac{\mathsf{K}^{(k)}}{A(\mathfrak{S}^{(i)})}\right)_2\right) \quad (i = 1, \ldots, e_2+1;\, k = 1, \ldots, e_2)$$

aufgestellt haben, wobei jetzt die $\mathsf{K}^{(k)}$ und $\mathfrak{S}^{(i)}$ je eine Basis von $\mathfrak{M}_2$ bzw. $\mathfrak{S}_1$ bilden. Wir haben vor allem die Elemente von M_2 zu berechnen. Das werden wir jetzt mit einer leichten Modifikation des bei (166), (167) geschilderten Verfahrens machen. Betrachten wir ein beliebiges Element

(179) $$\left(\frac{\mathsf{K}}{A(\mathfrak{S})}\right)_2 \quad (\mathsf{K} = \Omega(\sqrt{D_0}),\, \mathfrak{S} = (d', d'', 1, 1))$$

von M_2. Aus seiner Existenz folgt nach [8] Satz 5, daß alle

(180) $$\left(\frac{\mathsf{K}}{A(\mathfrak{T})}\right) \quad \left(\mathfrak{T} = \left(q_i, \frac{d}{q_i}, 1, 1\right);\ i = 1, \ldots, t\right)$$

gleich 1 sind. Da das Ideal $(\sqrt{q_i})$ in $A(\mathfrak{T})$ liegt, so bedeutet das, daß $(\sqrt{q_i})$ in $\mathsf{K}|\Omega$ voll zerfällt, d. h. q_i in K lauter Primidealfaktoren ersten Grades hat $(i = 1, \ldots, t)$. Indem wir also berücksichtigen, daß $(\sqrt{d'})$ in $A(\mathfrak{S})$ liegt, folgt ähnlich zu (166)

(181) $$\left(\frac{\mathsf{K}}{A(\mathfrak{S})}\right)_2 = \left(\frac{\alpha_1 | \mathsf{K}}{\mathfrak{a}}\right),$$

wobei $\mathfrak{a}$ ein beliebiges ganzes Ideal in K mit $N_{\mathsf{K}}\mathfrak{a} = d'$ bezeichnet und α_1 eine Zahl aus Satz 6 ist. Diese läßt sich jetzt in der Form

(182) $$\alpha = a + b\sqrt{D_0}$$

[47] Insbesondere für $m=1$ tritt dieser Fall unerwartet oft (und zwar — in asymptotischem Sinne — fast in der Hälfte aller Fälle) ein. Hierüber s. meine Arbeit [15]. Für beliebige m fehlen noch die entsprechenden Untersuchungen.

annehmen, wobei a, b mit c zusammen eine Lösung von

(183) $$a^2 = D_0 b^2 + D_0' c^2 \qquad (a, b, c \in [\mathrm{P}])$$

bilden, unterworfen den Nebenbedingungen

(184) $$(a, b, c) = 1, \quad 2 \mid b, \quad a + b \equiv 1 \pmod 4.$$

Offenbar ist

$$\mathfrak{a} = \mathfrak{b}\mathfrak{c}$$

ein passendes Ideal, wobei

$$\mathfrak{b} = (a - b\sqrt{D_0}, \sqrt{d'}), \quad \mathfrak{c} = (a - c\sqrt{D_0'}, \sqrt{d'})$$

ist. Da ferner

$$2(a + b\sqrt{D_0})(a + c\sqrt{D_0'}) = (a + b\sqrt{D_0} + c\sqrt{D_0'})^2$$

ist, so gilt nach (181), (182)

$$\left(\frac{\mathrm{K}}{A(\mathfrak{S})}\right)_2 = \left(\frac{a + b\sqrt{D_0} \mid \mathrm{K}}{\mathfrak{b}}\right) \left(\frac{2(a + c\sqrt{D_0'}) \mid \mathrm{K}}{\mathfrak{c}}\right)$$

also (nach Umkehrung der Reihenfolge der Faktoren)

(185) $$\left(\frac{\mathrm{K}}{A(\mathfrak{S})}\right)_2 = \left(\frac{a}{(D_0, d')}\right) \left(\frac{2a}{(D_0', d')}\right),$$

wobei die Faktoren der rechten Seite Jacobische Symbole sind. Mit Hilfe dieser Formel läßt sich M_2 bequem berechnen, und dann läßt sich der e_3-Schritt des Algorithmus ausführen.

Als einfaches Beispiel betrachten wir eine kritische Zahl

(186) $$D = pq$$

mit primären positiven Primzahlfaktoren p, q und nehmen

$$\left(\frac{p}{q}\right) = 1$$

d. h. $e_2 = 1$ an. Jetzt gibt es nur ein K. Hierfür läßt sich

$$\mathrm{K} = \Omega(\sqrt{p})$$

setzen. Für eine Basis von $(\mathfrak{S} =) \mathfrak{S}_1$ kann man

$$\mathfrak{S}^{(1)} = (p, q, 1, 1), \quad \mathfrak{S}^{(2)} = (q, p, 1, 1)$$

nehmen. Dann lautet (178) so:

(187) $$M_2 = \begin{pmatrix} \left(\frac{\mathrm{K}}{A(\mathfrak{S}^{(1)})}\right)_2 \\ \left(\frac{\mathrm{K}}{A(\mathfrak{S}^{(2)})}\right)_2 \end{pmatrix},$$

ferner läßt sich für (183)

(188) $$a^2 = pb^2 + qc^2$$

schreiben. Nach (185), (187) gilt jetzt

$$M_2 = \left|\begin{matrix} \left(\frac{a}{p}\right) \\ \left(\frac{2a}{q}\right) \end{matrix}\right|.$$

Mit Hilfe des Dirichletschen Symbols $\left(\frac{u}{v}\right)_4$ (s. [8] § 1) berechnen wir aus (188), (184) nach DIRICHLET:

$$\left(\frac{a}{p}\right)=\left(\frac{a^2}{p}\right)_4=\left(\frac{qc^2}{p}\right)_4=\left(\frac{q}{p}\right)_4\left(\frac{c}{p}\right)=\left(\frac{q}{p}\right)_4\left(\frac{p}{c}\right)=\left(\frac{q}{p}\right)_4,$$

$$\left(\frac{2a}{q}\right)=\left(\frac{2}{q}\right)\left(\frac{a^2}{q}\right)_4=\left(\frac{2}{q}\right)\left(\frac{p}{q}\right)_4\left(\frac{b}{q}\right)=\left(\frac{p}{q}\right)_4,$$

da man sieht, daß $\left(\frac{2b}{q}\right)=\left(\frac{q}{2b}\right)=1$ ist. Hiernach lautet (189) so:[48]

$$M_2 = \left|\begin{matrix} \left(\frac{q}{p}\right)_4 \\ \left(\frac{p}{q}\right)_4 \end{matrix}\right|.$$

Folglich gelten für den betrachteten Spezialfall die folgenden: Dann und nur dann ist $e_3 = 1$, wenn

(189) $$\left(\frac{p}{q}\right)_4=\left(\frac{q}{p}\right)_4=1$$

ist. In diesem Fall ist

$$px^2-qy^2=z^8 \qquad ((x, y, z)=1,\ 2\nmid z)$$

lösbar. Gilt

$$\left(\frac{p}{q}\right)_4=\left(\frac{q}{p}\right)_4=-1, \quad \text{bzw.} \quad \left(\frac{p}{q}\right)_4\neq\left(\frac{q}{p}\right)_4,$$

so ist

$$x^2-pqy^2=-1$$

lösbar bzw. unlösbar.[49]

In dem jetzt betrachteten Fall (186) haben wir alle Probleme I bis IV beantwortet, ausgenommen wenn (189) gilt. Endlich wollen wir für diesen Fall das einfache numerische Beispiel

$$D=149\cdot 17\,(=2533) \qquad \left(\left(\frac{149}{17}\right)_4=\left(\frac{17}{149}\right)_4=1\right)$$

betrachten. Dieses Beispiel wollen wir mit Anwendung des Zusatzes von

[48] Im obigen haben wir ein Beispiel vor uns, wo ein bedingtes Artinches Symbol einem Dirichletschen Symbol gleich ist. (Vgl. [8] § 1.)

[49] Viel allgemeinere Sätze obiger Art (bezüglich der Pellschen Gleichung auch für $m \neq 1$) finden sich bei RÉDEI [13], [14]. Vgl. auch SCHOLZ [23], RÉDEI [15], [17]. Alle Sätze in diesen Arbeiten lassen sich natürlich aus unseren vorliegenden Resultaten herleiten.

Satz 6 untersuchen. Man setze hierzu

$$n=2,\ D_0=149,\ D_0'=17.$$

Für (96) kann man

$$\alpha_1=49+4\sqrt{149}$$

nehmen, da hierfür

$$\alpha_1\alpha_1'=49^2-149\cdot 4^2=17\cdot 1^2 \tag{190}$$

gilt. Die Gleichung (97) lautet

$$\varrho^2+17\sigma^2=98\tau^2.$$

Man findet die Lösungen

$$\varrho=\pm 9,\ \sigma=\pm 1,\ \tau=\pm 1.$$

(Die Vorzeichen wählen wir unten passend.) In (98) gilt jetzt $\zeta=1$. Die rechte Seite von (99) ist gleich

$$98\tau+(\varrho+(49-4\sqrt{149})\sigma)\sqrt{\alpha_1}.$$

Diese Zahl ist durch 2 teilbar. Wir wählen $\varrho=-9$, $\sigma=1$, $\tau=-1$ und dividieren durch 2. Die erhaltene Zahl

$$\alpha_2=-49+(20-2\sqrt{149})\sqrt{\alpha_1} \tag{191}$$

befriedigt dann (91) und wegen

$$\alpha_2\equiv 1 \pmod 4$$

zugleich auch (93). Ferner gilt

$$\alpha_2\alpha_2'=(29+2\sqrt{149})^2\alpha_1'. \tag{192}$$

Da jetzt wegen (190)

$$\mathfrak{d}_1=\alpha_1 \qquad (\mathfrak{d}_1|17)$$

gesetzt werden kann, so folgt aus (192) (wegen $29^2-149.2^2=5.7^2$), daß mit

$$\mathfrak{d}_2=(\alpha_2,\alpha_1') \tag{193}$$

auch (92), (95) befriedigt sind. Hiernach braucht man den Teil II des Zusatzes gar nicht anzuwenden. Auch die Anwendung des Teils III ist unnötig, da — wie man leicht nachrechnet — auch (94) befriedigt ist. Wir haben also

$$\mathrm{K}_3=\mathrm{K}_2(\sqrt{\alpha_2})\ (=\Omega(\sqrt{149},\sqrt{\alpha_1},\sqrt{\alpha_2})). \tag{194}$$

Mit $\mathfrak{P}$ und $\mathfrak{Q}$ bezeichnen wir je ein Primideal in K_2 mit

$$\mathfrak{P}|149,\quad \mathfrak{Q}|17.$$

(Beide sind also vom ersten Grade.) Dann läßt sich

$$M_2=\begin{pmatrix}\left(\dfrac{\alpha_2|\mathrm{K}_2}{\mathfrak{P}}\right)\\ \left(\dfrac{\alpha_2|\mathrm{K}_2}{\mathfrak{Q}}\right)\end{pmatrix} \tag{195}$$

setzen. Da $\alpha_1\equiv 49 \pmod{\mathfrak{P}}$ ist, so gilt nach passender Wahl von $\mathfrak{P}$

$$\sqrt{\alpha_1}\equiv 7 \pmod{\mathfrak{P}},\ \alpha_2\equiv 91 \pmod{\mathfrak{P}}.$$

Folglich ist (nach (167)

$$\left(\frac{\alpha_2|K_2}{\mathfrak{P}}\right)=\left(\frac{91}{149}\right)=-1.$$

Für $\mathfrak{Q}$ läßt sich

$$\mathfrak{Q}=(17,\alpha_2')$$

nehmen. Dann gilt nach (191)

$$\left(\frac{\alpha_2|K_2}{\mathfrak{Q}}\right)=\left(\frac{\alpha_2+\alpha_2'|K_2}{\mathfrak{P}}\right)=\left(\frac{98|K_2}{\mathfrak{P}}\right)=\left(\frac{98}{17}\right)=1.$$

Nach Einsetzung in (195) haben wir

$$M_3=\begin{pmatrix} -1 \\ 1 \end{pmatrix}.$$

Hiernach ist M_3 schon ausreduziert. Die Anwendung der Sätze 1, 3 ergibt, daß $e_4=0$ $(\nu=3)$ und die Pellsche Gleichung

$$x^2-149.17y^2=-1$$

unlösbar ist. Ferner folgt aus den Sätzen 2, 3, daß

$$17x^2-149y^2=z^{16} \qquad ((x,y,z)=1,\ 2\nmid z)$$

und sogar die Dirichletsche Gleichung

$$17x^2-149y^2=1$$

lösbar ist. In der Tat findet man

$$17.225^2-149.76^2=1.$$

(Eingegangen am 10. Juli 1953.)

Literaturverzeichnis

[1] G. L. Dirichlet, Einige neue Sätze über unbestimmte Gleichungen, *Ges. Werke,* I (Berlin, 1889), S. 221—236.

[2] P. Epstein, Zur Auflösbarkeit der Gleichung $x^2-Dy^2=-1$, *Journ. f. reine u. angew. Math.,* **171** (1934), S. 243—252.

[3] H. Hasse, Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, Teil I, Ia, II, *Jahresb. d. Deutsch. Math. Ver.,* **35** (1926), S. 1—55; **36** (1927), S. 233—311; Ergänzungsband **6** (1930), S. 1—204.

[4] E. Inaba, Über die Struktur der *l*-Klassengruppe zyklischer Zahlkörper vom Primzahlgrad *l*, *Journ. Fac. Sci. Univ. Tokyo,* Sect. II, **4** (1940), S. 61—115.

[5] S. Iyanaga, Sur les classes d'idéaux dans les corps quadratiques, *Actualitées scient. et ind.,* Nr. **197** (1935), S. 3—13.

[6] T. Nagell, Über die Lösbarkeit der Gleichung $x^2-Dy^2=-1$, *Arkiv för Mat., Astr. o. Fysik,* **23** B/6 (1932), S. 1—5.

[7] W. Patz, *Tafel der regelmäßigen Kettenbrüche für Quadratwurzeln aus den natürlichen Zahlen von* 1—10000 (Leipzig, 1941).

[8] L. Rédei, Bedingtes Artinsches Symbol mit Anwendung in der Klassenkörpertheorie, *Acta Math. Acad. Sci. Hung.*, **4** (1953), S. 1—29 (die vorstehende Arbeit).

[9] L. Rédei, Die Anzahl der durch vier teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers, *Math. u. Naturwiss. Anz. d. Ung. Akad. d. Wiss.*, **49** (1932), S. 338—363 (in ungarischer Sprache mit deutschem Auszug).

[10] L. Rédei und H. Reichardt, Die Anzahl der durch 4 teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers, *Journ. f. reine u. angew. Math.*, **170** (1933), S. 69—74.

[11] L. Rédei, Arithmetischer Beweis des Satzes über die Anzahl der durch vier teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper, *Journ. f. reine u. angew. Math.*, **171** (1934), S. 55—60.

[12] L. Rédei, Eine obere Schranke der Anzahl der durch vier teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper, *Journ. f. reine u. angew. Math.*, **171** (1934), S. 61—64.

[13] L. Rédei, Über die Grundeinheit und die durch 8 teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper, *Journ. f. reine u. angew. Math.*, **171** (1934), S. 131—148.

[14] L. Rédei, Über die Pellsche Gleichung $t^2-du^2=-1$, *Journ. f. reine u. angew. Math.*, **173** (1935), S. 193—211.

[15] L. Rédei, Über einige Mittelwertfragen im quadratischen Zahlkörper, *Journ. f. reine u. angew. Math.*, **174** (1935), S. 15—55.

[16] L. Rédei, Über die *D*-Zerfällungen zweiter Art, *Math. u. Naturwiss. Anz. der Ung. Akad. d. Wiss.*, **56** (1937), S. 89—125 (in ungarischer Sprache mit deutschem Auszug).

[17] L. Rédei, Ein neues zahlentheoretisches Symbol mit Anwendungen auf die Theorie der quadratischen Zahlkörper, I, *Journ. f. reine u. angew. Math.*, **180** (1938), S. 1—43.

[18] L. Rédei, Die Diophantische Gleichung $mx^2+ny^2=z^4$, *Monatshefte f. Math.*, **48** (1939), S. 43—60.

[19] L. Rédei, Über die Klassengruppen und Klassenkörper algebraischer Zahlkörper, *Journ. f. reine u. angew. Math.*, **186** (1944), S. 80—90.

[20] L. Rédei, Bemerkung zu einer Arbeit von R. Fueter über die Klassenkörpertheorie, *Acta Sci. Math.* (Szeged), **11** (1947), S. 37—38.

[21] L. Rédei, Über den geraden Teil der Ringklassengruppe von quadratischen Zahlkörpern, die Pellsche Gleichung und die Diophantische Gleichung $rx^2+sy^2=z^{2^n}$, I, II, III, *Math. u. Naturwiss. Anz. d. Ung. Akad. d. Wiss.*, **62** (1943), S. 13—34; S. 35—47; S. 48—62. (Ungarisch mit deutschem Auszug.)

[22] H. Reichardt, Zur Struktur der absoluten Idealklassengruppe im quadratischen Zahlkörper, *Journ. f. reine u. angew. Math.*, **170** (1933), S. 75—82.

[23] A. Scholz, Über die Lösbarkeit der Gleichung $t^2-Du^2=-4$, *Math. Zeitschrift*, **39** (1934), S. 93—111.

[24] F. Tano, Sur quelques théorèmes de Dirichlet, *Journ. f. reine u. angew. Math*, **105** (1889), S. 160—169.

2-ГРУППА КЛАССОВ АЛГЕБРАИЧЕСКИХ ПОЛЕЙ ВТОРОГО ПОРЯДКА И ТЕОРИЯ УРАВНЕНИЯ ПЭЛЛА

Л. РЭДЭИ (Сегед)

(Резюме)

Эта работа — применение предыдущей работы автора к тому специальному случаю, когда исходное числовое поле Ω — алгебраическое поле второго порядка, а группа классов $\mathfrak{H}$ есть 2-группа классов колец поля Ω mod. m (m — нечётное целое число). Находятся её инварианты и, в связи с этой проблемой, полностью исследуется старая проблема о существовании решений уравнения Пэлла

$$x^2-dm^2y^2=-1.$$

Оказывается, что эти проблемы находятся в такой тесний связи друг с другом, и что в сущности речь идёт об эквивалентных проблемах. Решение является завершением относящихся сюда исследований Гаусса и Дирихле и даёт доброиспользуемые ответы на оба вопроса. (Напротив, известный критерий „цепных дробей" во многих отношениях не удовлетворителен.) Решается также вопрос о существовании решения для диофантовых уравнений вида

$$d'm'^2x'^2-d''m''^2x''^2=1,\quad d'm'^2x'^2-d''m''x''^2=z^2,$$

в тесной связи с предыдущими.

ÜBER DIE NICHTREELLEN WERTE EINER TOTALREELLEN RATIONALEN FUNKTION

Von

GYULA SZ.-NAGY (Szeged), Mitglied der Akademie

1. Eine rationale Funktion n-ten Grades,

$$F(z)=\frac{g(z)}{f(z)}=\frac{\beta_0 z^n+\beta_1 z^{n-1}+\cdots+\beta_n}{\alpha_0 z^n+\alpha_1 z^{n-1}+\cdots+\alpha_n}, \qquad |\alpha_0|+|\beta_0|\neq 0, \tag{1}$$

($g(z)$ und $f(z)$ haben keine gemeinsame Nullstelle) wurde von mir *totalreell*[1] genannt, wenn sie außerhalb der reellen Achse in keinem Punkt der komplexen Ebene einen reellen Wert besitzt. Ich habe bewiesen: Ist $F(z)$ totalreell, so haben die Polynome $f(z)$ und $g(z)$ lauter reelle Nullstellen und die Nullstellen des einen Polynoms werden von denjenigen des anderen getrennt. Haben die Nullstellen der Polynome $f(z)$ und $g(z)$ mit lauter reellen Koeffizienten diese Eigenschaften, so ist die rationale Funktion $F(z)$ totalreell.

Es gilt nun der Satz:

I. *Die totalreelle rationale Funktion n-ten Grades*

$$F(z)=\prod_{k=1}^{n}\frac{z-b_k}{z-a_k}, \qquad a_1<b_1<a_2<b_2<\cdots<a_n<b_n \tag{2}$$

hat außerhalb des Kreises K_0 mit dem Durchmesser (a_1, b_n) in jedem Punkt einen positiven Realteil und in den inneren Punkten der Kreise $K_h (h=1,2,\ldots,n)$ mit den Durchmessern (a_h, b_h) einen negativen Realteil. Die Punkte der komplexen Ebene, in denen diese Funktion $F(z)$ rein imaginär ist, liegen auf einer algebraischen Kurve $2n$-ter Ordnung mit der Gleichung $\operatorname{Re} F(z)=0$, *die sich auch in der Form*

$$\operatorname{Re} F(z)=1+\operatorname{Re}\sum_{k=1}^{n}\frac{A_k}{z-a_k}=1+\sum_{k=1}^{n}\frac{A_k(x-a_k)}{(x-a_k)^2+y^2}=0 \quad (z=x+iy) \tag{3}$$

schreiben läßt, wo

$$A_k=\frac{g(a_k)-f(a_k)}{f'(a_k)} \qquad (k=1,2,\ldots,n).$$

[1] Gy. Sz.-Nagy, Totalreelle rationale Funktionen, *Acta Scient. Math. Szeged*, **12 A** (1950), S. 1—10.

2. Sind

$$\varphi_k = \operatorname{arc}\frac{z-b_k}{z-a_k}, \quad \psi_k = \operatorname{arc}\frac{z-a_{k+1}}{z-b_k}, \quad |\varphi_k| \leqq \pi, \quad |\psi_k| \leqq \pi,$$
$$(k=1,2,\ldots,n;\ a_{n+1}\equiv a_1),$$

so bedeutet φ_k bzw. ψ_k den Winkel, unter dem der Vektor $\overrightarrow{a_k b_k}$ bzw. $\overrightarrow{b_k a_{k+1}}$ vom Punkt z aus erscheint. Wegen der Aufeinanderfolge der Punkte a_k und b_k auf der reellen Achse haben die Vektoren $\overrightarrow{a_k b_k}$ $(k=1,2,\ldots,n)$, $\overrightarrow{a_1 b_n}$ und $\overrightarrow{b_k a_{k+1}}$ $(k=1,2,\ldots,n-1)$ dieselbe Richtung. Folglich haben die Winkel

$$\varphi_1, \varphi_2, \ldots, \varphi_n;\ \psi_1, \psi_2, \ldots, \psi_{n-1} \quad \text{und} \quad \Psi \equiv -\psi_n$$

denselben Drehungssinn, der positiv bzw. negativ ist, je nachdem der Punkt z oberhalb bzw. unterhalb der reellen Achse liegt. Aus der Vektorgleichung

$$\overrightarrow{a_1 b_n} = \overrightarrow{a_1 b_1} + \overrightarrow{b_1 a_2} + \cdots + \overrightarrow{b_{n-1} a_n} + \overrightarrow{a_n b_n}$$

folgt die Winkelgleichung

$$\Psi = \varphi_1 + \psi_1 + \varphi_2 + \psi_2 + \cdots + \psi_{n-1} + \varphi_n = \sum_{k=1}^{n} \varphi_k + \sum_{k=1}^{n-1} \psi_k \equiv \Phi + \Psi'.$$

Hieraus ergibt sich die Gleichung

$$\operatorname{arc} F(z) = \sum_{k=1}^{n} \operatorname{arc}\frac{z-b_k}{z-a_k} = \sum_{k=1}^{n} \varphi_k = \Phi = \Psi - \Psi'. \tag{4}$$

Es genügt offenbar den Satz I nur für die Punkte z der oberen komplexen Halbebene zu beweisen, weil die reelle Funktion $F(z)$ in konjugiert komplexen Stellen z und $\bar{z}$ denselben Realteil besitzt. Für jeden Punkt z oberhalb der reellen Achse sind die Winkel $\varphi_1, \varphi_2, \ldots, \varphi_n$, $\psi_1, \psi_2, \ldots, \psi_{n-1}$ und $\Psi < \pi$ positiv, weil Ψ den Winkel bedeutet, unter dem der Vektor $\overrightarrow{a_1 b_n}$ vom Punkt z aus erscheint.

In einem Punkt z der oberen Halbebene, der auf dem Kreis K_0 bzw. außerhalb von K_0 liegt, ist $\Psi = \frac{\pi}{2}$ bzw. $\Psi < \frac{\pi}{2}$. Folglich ist $\operatorname{Re} F(z) > 0$, weil $0 < \Phi < \Psi \leqq \frac{\pi}{2}$ ist.[2]

Liegt aber der Punkt z der oberen Halbebene auf oder in dem Kreis K_h, so ist $\varphi_h \geqq \frac{\pi}{2}$. Hieraus folgt die Ungleichung $\operatorname{Re} F(z) < 0$, weil $\pi > \Phi > \varphi_h \geqq \frac{\pi}{2}$ ist.

[2] Für die Punkte des Kreises K_0 ist unser Beweis ähnlich zu den Beweisen der Arbeit von C. Colombo, Intorno alle distribuzione degli zeri di certi Polinomi, *Atti Acad. Naz. Lincei,* (3), 8 (1847), S. 530—535.

Liegt der Punkt z_0 bzw. z_h auf dem Kreis K_0 bzw. K_h, so enthält die Strecke $z_0 z_h$ mindestens einen Punkt z, in dem $\Phi = \frac{\pi}{2}$, also $\operatorname{Re} F(z) = 0$ ist. Während nämlich ein Punkt z von z_0 ausgehend die Strecke $z_0 z_h$ beschreibt, verändert sich die Funktion $\operatorname{arc} F(z)$ von $\operatorname{arc} F(z_0) < \frac{\pi}{2}$ ausgehend bis $\operatorname{arc} F(z_h) > \frac{\pi}{2}$ stetig.

Die Form der Gleichung (3) folgt aus der Partialbruchzerlegung der Funktion

$$(5) \qquad F(z) = \frac{g(z)}{f(z)} = 1 + \frac{g(z) - f(z)}{f(z)} = 1 + \sum_{k=1}^{n} \frac{A_k}{z - a_k}.$$

Damit is der Satz I bewiesen.

In jedem Punkt z der oberen Halbebene hat die Funktion $F(z)$ einen positiven Imaginärteil, weil im Punkt z $0 < \Phi < \pi$ ist.

3. Ist $F(z) = |F(z)| e^{i\vartheta}$ $(F(z) \neq 0,\ 0 \leqq |\vartheta| \leqq \pi)$, so sagen wir, daß die Funktion $F(z)$ im Punkt z den Winkel ϑ besitzt.

Es gilt die folgende Verallgemeinerung des Satzes I.

II. *Bezeichnet K_0' bzw. K_h' $(h = 1, 2, \ldots, n)$ den Kreis, von dessen Punkten aus der Vektor $\overrightarrow{a_1 b_0}$ bzw. $\overrightarrow{a_h b_h}$ unter dem Winkel ϑ $(0 \leqq \vartheta \leqq \pi)$ erscheint, so hat die Funktion $F(z)$ außerhalb des Kreises K_0' in einem Punkt z einen Winkel $< \vartheta$ bzw. $> \vartheta - \pi$, je nachdem* $\operatorname{Im} z > 0$ *bzw.* $\operatorname{Im} z < 0$ *ist. In einem inneren Punkt z des Kreises K_h' ist der Winkel der Funktion $F(z) > \vartheta$ bzw. $< \vartheta - \pi$, je nachdem* $\operatorname{Im} z > 0$ *bzw.* $\operatorname{Im} z < 0$ *ist.*

Dieser Satz läßt sich ebenso einsehen, wie der Satz I. In einem Punkt z außerhalb des Kreises K_0' ist $\psi < \vartheta$ bzw. $0 > \psi > \vartheta - \pi$, also $\operatorname{arc} F(z) = \Phi < \Psi < \vartheta$ bzw. $\Phi > \vartheta - \pi$, je nachdem $\operatorname{Im} z > 0$ bzw. $\operatorname{Im} z < 0$ ist. In einem inneren Punkt z des Kreises K_h' ist $\varphi_h > \vartheta$ bzw. $\varphi_h < \vartheta - \pi$, also $\Phi > \varphi_h > 0$ bzw. $\Phi < \varphi_h < \vartheta - \pi$, je nachdem $\operatorname{Im} z > 0$ bzw. $\operatorname{Im} z < 0$ ist. Damit ist der Satz II bewiesen.

Die Punkte z der komplexen Ebene, in denen die Funktion $F(z)$ den Winkel ϑ oder $\vartheta - \pi$ besitzt, liegen auf einer algebraischen Kurve $2n$-ter Ordnung, deren Gleichung die Form

$$(6) \qquad \sin\vartheta \operatorname{Re} F(z) - \cos\vartheta \operatorname{Im} F(z) = 0$$

oder nach (5) die Form

$$1 + \sum_{k=1}^{n} \frac{(x - a_k)\sin\vartheta - y\cos\vartheta}{(x - a_k)^2 + y^2} = 0$$

besitzt. Hat nämlich $F(z)$ im Punkt z den Winkel ϑ bzw. $\vartheta - \pi$, so sind

$\operatorname{Re} F(z) = |F(z)| \cos \vartheta$, $\operatorname{Im} F(z) = |F(z)| \sin \vartheta$ bzw. $\operatorname{Re} F(z) = -|F(z)| \cos \vartheta$. $\operatorname{Im} F(z) = -|F(z)| \sin \vartheta$. Die Gleichung (6) besteht also in beiden Fällen.

4. Est gilt auch der Satz:

III. *Bezeichnet* K_0'' *bzw.* K_h'' $(h = 1, 2, \ldots, n)$ *das Kreiszweieck, von dessen Randpunkten aus die Strecke* $a_1 b_n$ *bzw.* $a_h b_h$ *unter dem Winkel* ω $(0 < \omega < \pi)$ *erscheint und bedeutet* $F(z)$ *die totalreelle rationale Funktion* (2), *so besteht in jedem Punkt* z *außerhalb des Kreiszweiecks* K_0'', *bzw. in jedem inneren Punkt* z *des Kreiszweiecks* K_h'' $(h = 1, 2, \ldots, n)$ *die Ungleichung* $|\operatorname{arc} F(z)| < \omega$ *bzw.* $|\operatorname{arc} F(z)| > \omega$.

Die Punkte z der komplexen Ebene, in denen $|\operatorname{arc} F(z)| = \omega$ ist, bilden eine geschlossene Kurve, die aber im Falle $\omega \neq \pi - \omega$ keine vollständige algebraische Kurve ist. Sie ist bezüglich der reellen Achse symmetrisch und ihre oberhalb bzw. unterhalb der reellen Achse liegenden Punkte gehören zu der Kurve (6) bei $\vartheta = \omega$ bzw. $\vartheta = \pi - \omega$. Die Kurve $|\operatorname{arc} F(z)| = \frac{\pi}{2}$ stimmt mit der Kurve (3) überein. Der Satz III läßt sich ebenso einsehen, wie die Sätze I und II.

5. Aus dem Beweis des Satzes folgt die Verallgemeinerung von I:

IV. *Genügen die positiven Zahlen* a_h *und* b_h *den Ungleichungen*

$$0 < a_h < b_h < a_{h+1} \qquad (h = 1, 2, \ldots)$$

und ist die unendliche Reihe $\sum_{h=1}^{\infty} a_h^{-1}$ *konvergent, so ist der Realteil der Funktion*

$$F(z) = \frac{g(z)}{f(z)}, \quad f(z) = \prod_{h=1}^{\infty} \left(1 - \frac{z}{a_h}\right), \quad g(z) = \prod_{h=1}^{\infty} \left(1 - \frac{z}{b_h}\right)$$

in den Punkten der Halbebene $\operatorname{Re} z < a_1$ *positiv und in den inneren Punkten der Kreise* K_h *mit den Durchmessern* (a_h, b_h) $(h = 1, 2, \ldots)$ *negativ.*

$f(z)$ und $g(z)$ sind ganze Funktionen vom Geschlecht Null. Die Funktion $F(z)$ hat die Form

$$F(z) = \prod_{h=1}^{\infty} \frac{1 - \dfrac{z}{b_h}}{1 - \dfrac{z}{a_h}} = \prod_{h=1}^{\infty} \frac{a_h}{b_h} \frac{z - b_h}{z - a_h}.$$

Folglich ist

$$\operatorname{arc} F(z) = \sum_{h=1}^{\infty} \operatorname{arc} \left(\frac{a_h}{b_h} \frac{z - b_h}{z - a_h}\right) = \sum_{h=1}^{\infty} \operatorname{arc} \frac{z - b_h}{z - a_h} = \sum_{h=1}^{\infty} \varphi_h = \Phi < \Psi < \pi.$$

6. Im Satz IV ist $F(z)$ eine Grenzfunktion von totalreellen rationalen Funktionen. Im folgenden Satz ist $G(z)$ eine Grenzfunktion von reellen rationalen Funktionen, die auch auf der imaginären Achse reelle Werte besitzen.

V. *Sind* $0 < a_h < b_h < a_{h+1}$ $(h = 1, 2, \ldots)$, *ist die Reihe* $\sum_{h=1}^{\infty} a_h^{-2}$ *konvergent und ist*

$$G(z) = \prod_{h=1}^{\infty} \left(\frac{a_h}{b_h}\right)^2 \frac{z^2 - b_h^2}{z^2 - a_h^2}, \tag{7}$$

so ist $\operatorname{Im} G(z) > 0$, $\operatorname{Im} G(z) < 0$ *bzw.* $\operatorname{Im} G(z) = 0$, *je nachdem* $\operatorname{Re} z \operatorname{Im} z > 0$ $\operatorname{Re} z \operatorname{Im} z < 0$, *bzw.* $\operatorname{Re} z \operatorname{Im} z = 0$ *ist.*

Aus (7) folgt die Gleichung

$$\operatorname{arc} G(z) = \sum_{h=1}^{\infty} \left(\operatorname{arc} \frac{z - b_h}{z - a_h} + \operatorname{arc} \frac{z + b_h}{z + a_h} \right) = \sum_{h=1}^{\infty} (\varphi_h + \psi_h), \quad |\varphi_h| \leqq \pi, \quad |\psi_h| \leqq \pi.$$

Hier bedeutet φ_h bzw. ψ_h den Winkel, unter dem der Vektor $\overrightarrow{a_h b_h}$ bzw. $\overrightarrow{(-a_h)(-b_h)}$ vom Punkt z aus erscheint.

In einem Punkt z außerhalb der reellen Achse haben die Winkel φ_h und ψ_h $(h = 1, 2, \ldots)$ offenbar entgegengesetzte Vorzeichen. Liegt z auf der imaginären Achse, so sind $\varphi_h + \psi_h = 0$ und $\operatorname{arc} G(z) = 0$. Der Wert $G(z)$ ist also in den Punkten der imaginären Achse positiv.

Für einen Punkt z außerhalb beider Achsen sieht man leicht ein, daß $|\varphi_h| > |\psi_h|$ bzw. $|\varphi_h| < |\psi_h|$ ist, falls $\operatorname{Re} z > 0$ bzw. $\operatorname{Re} z < 0$ ist und daß $\varphi_h > 0$ bzw. $\varphi_h < 0$ ist, falls $\operatorname{Im} z > 0$ bzw. $\operatorname{Im} z < 0$ ist.

Besteht also die Ungleichung $\operatorname{Re} z \operatorname{Im} z > 0$ bzw. $\operatorname{Re} z \operatorname{Im} z < 0$, so ist jede Summe $\varphi_h + \psi_h$ positiv bzw. negativ. Im Falle $\operatorname{Re} z \operatorname{Im} z > 0$ bzw. $\operatorname{Re} z \operatorname{Im} z < 0$ ist also

$$0 < \operatorname{arc} G(z) = \sum_{h=1}^{\infty} (\varphi_h + \psi_h) < \pi \quad \text{bzw.} \quad 0 > \operatorname{arc} G(z) > -\pi,$$

weil offenbar

$$\left| \sum_{h=1}^{\infty} \varphi_h \right| = \sum_{h=1}^{\infty} |\varphi_h| < \pi \quad \text{und} \quad \left| \sum_{h=1}^{\infty} \psi_h \right| = \sum_{h=1}^{\infty} |\psi_h| < \pi$$

sind.

Daraus folgt der Satz, weil er für den Fall $\operatorname{Re} z \operatorname{Im} z = 0$ schon bewiesen wurde.

(Eingegangen am 15. Dezember 1952.)

О НЕВЕЩЕСТВЕННЫХ ЗНАЧЕНИЯХ ТОТАЛЬНО ВЕЩЕСТВЕННОЙ РАЦИОНАЛЬНОЙ ФУНКЦИИ

Д. С.-НАДЬ (Сегед)

(Резюме)

Рациональная функция n-ной степени

$$F(z)=\frac{g(z)}{f(z)}=\prod_{k=1}^{n}\frac{z-b_k}{z-a_k} \quad (a_1<b_1<a_2<b_2<\cdots<a_n<b_n)$$

—тотально вещественна, т. е. принимает вещественные значения лишь на оси абсцисс. Функция $F(z)$ в любой точки z плоскости, лежащей вне окружности K_0, диаметром которой служит отрезок (a_1, b_n), принимает значение, вещественная часть которого положительна. Внутри окружности K_h $(h=1, 2, \ldots, n)$, диаметром которой является отрезок (a_h, b_h), вещественная часть функции $F(z)$ отрицательна. Эту теорему можно обобщить и на частное от двух целых функций нулевого порядка.

ÜBER DEN EINFLUSS DER STRUKTUR EINER FUNKTION AUF DIE KONVERGENZ FAST ÜBERALL IHRER FOURIERREIHE

Von

G. ALEXITS (Budapest), Mitglied der Akademie

Einleitung

Das weitgehendste bis jetzt erreichte Resultat bezüglich der Konvergenz fast überall der Fourierreihe

$$\frac{a_0}{2}+\sum_{n=1}^{\infty}(a_n \cos nx + b_n \sin nx) \sim f(x) \tag{1}$$

ist der Satz von KOLMOGOROFF—SELIVERSTOFF[1] und PLESSNER,[2] nach welchem die Konvergenz fast überall der Reihe (1) eine Folge von

$$\sum_{n=1}^{\infty}(a_n^2+b_n^2)\log n < \infty \tag{2}$$

ist. Trotz der großen Bedeutung dieses Satzes ist wenig bekannt, welche strukturelle Eigenschaften der Funktion $f(x)$ das Erfülltsein von (2) sichern. Eine derartige Untersuchung wurde von PLESSNER[2] selbst begonnen, ihre Weiterführung wäre deshalb nötig, weil die bisher bekannten Sätze über den Einfluß der strukturellen Eigenschaften einer Funktion auf die Konvergenzverhältnisse ihrer Fourierreihe schon in den einfachsten Fällen versagen. Es scheint z. B. nicht einmal bekannt zu sein, wie sich die Konvergenzverhältnisse der Fourierreihe (1) gestalten, wenn die Funktion $f(x)$ zwar einer Dini—Lipschitzschen Bedingung α-ter Ordnung genügt ($\alpha < 1$), jedoch die Dini—Lipschitzsche Bedingung schlechthin in keinem Teilintervall von $(0, 2\pi)$ erfüllt ist.

Im folgenden soll gezeigt werden, daß man durch Betrachtung des sogenannten quadratischen Stetigkeitsmoduls

$$\omega_2(\delta, f) = \sup_{|h|\leq\delta}\left\{\int_0^{2\pi}[f(x+h)-f(x)]^2dx\right\}^{\frac{1}{2}}$$

[1] A. KOLMOGOROFF—G. SELIVERSTOFF, Sur la convergence des séries de Fourier, *Comptes Rendus Acad. Sci. Paris,* **178** (1925), S. 303—305 und *Rendiconti Acad. Lincei Roma,* **3** (1926), S. 307—310.

[2] A. PLESSNER, Über Konvergenz von trigonometrischen Reihen, *Journal f. reine u. angew. Mathematik,* **155** (1926), S. 15—25.

eine strukturelle Konvergenzbedingung angeben kann, welche der Kolmogoroff—Seliverstoff—Plessnerschen Koeffizientenbedingung (2) vollkommen äquivalent ist. Wir werden nämlich den folgenden Satz beweisen:

SATZ 1. *Die Gültigkeit der Beziehung* (2) *ist mit der Behauptung gleichwertig, daß es eine positive monoton zunehmende Funktion* $\lambda(x)$ *mit*

$$\int_1^\infty \frac{dx}{x\lambda(x)} < \infty \tag{3}$$

gibt derart, daß die Beziehung

$$\omega_2(\delta, f) = O\left(\frac{1}{\sqrt{\lambda(1/\delta)}}\right) \tag{4}$$

besteht.

Dieses Resultat kann deshalb ein gewisses Interesse haben, weil es die Konvergenz fast überall der Fourierreihe direkt aus der Struktur der Funktion $f(x)$ abzulesen ermöglicht. Als einfache Anwendung soll nur darauf hingewiesen werden, daß nach unserem Satz $\omega_2(\delta, f) = O(\log 1/\delta)^{-\frac{1}{2}-\varepsilon}$ mit $\varepsilon > 0$, oder $\omega_2(\delta, f) = O((\log 1/\delta)^{-\frac{1}{2}}(\log\log 1/\delta)^{-\frac{1}{2}-\varepsilon})$, usw. die Konvergenz fast überall der Fourierreihe (1) sichert; eine Dini-Lipschitzsche Bedingung α-ter Ordnung mit $\alpha > \frac{1}{2}$ reicht also für die Konvergenz fast überall der Fourierreihe ausgiebig hin. Darüber hinaus scheint vielleicht auch der Umstand bemerkenswert zu sein, daß die im Satz 1 enthaltene Konvergenzbedingung leicht auf eine lokale Form gebracht werden kann. Bedeutet nämlich

$$\omega_2(\delta, f; a, b) = \sup_{|h| \leq \delta} \left\{\int_a^b [f(x+h) - f(x)]^2\, dx\right\}^{\frac{1}{2}},$$

so gilt auch der folgende

SATZ 2. *Ist die L-integrierbare Funktion* $f(x)$ *in einem Teilintervall* (a, b) *von* $(0, 2\pi)$ L^2*-integrierbar und gilt*

$$\omega_2(\delta, f; a, b) = O\left(\frac{1}{\sqrt{\lambda(1/\delta)}}\right), \tag{5}$$

wo die monoton zunehmende Funktion $\lambda(x)$ *die Bedingung* (3) *erfüllt, so ist die Fourierreihe* (1) *in* (a, b) *fast überall konvergent.*

Die lokale Konvergenzbedingung (5) verlangt außerhalb des Intervalls (a, b) überhaupt nicht die L^2-Integrierbarkeit von $f(x)$, sie kann daher auch dann angewendet werden, wenn die Reihe $\sum(a_n^2 + b_n^2)$ divergiert.

Beweis des Satzes 1

Wir beweisen erstens, daß aus (3) und (4) die Gültigkeit von (2) folgt. Wegen

$$f(x+h)-f(x-h)\sim 2\sum_{k=1}^{\infty}(b_k\cos kx-a_k\sin kx)\sin kh$$

gilt nämlich

$$(6)\qquad \sum_{k=1}^{\infty}(a_k^2+b_k^2)\sin^2 kh=\frac{1}{4\pi}\int_0^{2\pi}[f(x+h)-f(x-h)]^2\,dx\leq\frac{1}{\pi}[\omega_2(h,f)]^2.$$

Daraus ergibt sich[3]

$$\frac{1}{2}\sum_{k=1}^{\infty}(a_k^2+b_k^2)\left(1-\frac{\sin\frac{2k}{n}}{\frac{2k}{n}}\right)\leq n\int_0^{\frac{1}{n}}\frac{1}{\pi}[\omega_2(h,f)]^2\,dh\leq\frac{1}{\pi}\left[\omega_2\left(\frac{1}{n},f\right)\right]^2.$$

Beachten wir, daß für $k\geqq n$

$$1-\frac{\sin\frac{2k}{n}}{\frac{2k}{n}}\geqq\frac{1}{2}$$

und für $1\leqq k\leqq n$

$$1-\frac{\sin\frac{2k}{n}}{\frac{2k}{n}}\geqq 0$$

ist, so folgt

$$(7)\qquad \sum_{k=n}^{\infty}(a_k^2+b_k^2)\leqq\frac{4}{\pi}\left[\omega_2\left(\frac{1}{n},f\right)\right]^2.$$

Aus (3), (4) und (7) ergibt sich aber durch eine Abel-Transformation

$$\sum_{k=1}^{n-1}(a_k^2+b_k^2)\sum_{j=1}^{k}\frac{1}{j}+\sum_{k=n}^{\infty}(a_k^2+b_k^2)\cdot\sum_{j=1}^{n}\frac{1}{j}=\sum_{k=1}^{n}\frac{\sum_{j=k}^{\infty}(a_j^2+b_j^2)}{k}\leqq$$

$$\leqq\frac{4}{\pi}\sum_{n=1}^{\infty}\frac{\left[\omega_2\left(\frac{1}{n},f\right)\right]^2}{n}=O(1)\int_1^{\infty}\frac{dx}{x\lambda(x)}=O(1),$$

woraus man unmittelbar

$$\sum_{n=1}^{\infty}(a_n^2+b_n^2)\log n\leqq\sum_{n=1}^{\infty}(a_n^2+b_n^2)\sum_{j=1}^{n}\frac{1}{j}<\infty,$$

also die Gültigkeit von (2) abliest.

[3] Diese recht einfache Schlußweise verdanke ich einer mündlichen Mitteilung von A. Rényi.

Wir beweisen zweitens, daß man umgekehrt aus (2) die Beziehung (3) und (4) herleiten kann. Sei in der Tat n die größte ganze Zahl $\leqq \frac{1}{h}$, wo $h>0$. Dann gilt nach (6) die Abschätzung

$$\frac{1}{4\pi}\int_0^{2\pi}[f(x+h)-f(x-h)]^2\,dx \leqq \sum_{k=n}^{\infty}(a_k^2+b_k^2)+\frac{1}{n}\sum_{k=1}^{n}k^2(a_k^2+b_k^2).$$

Das rechtsstehende letzte Glied läßt sich folgenderweise umformen:

$$\frac{1}{n^2}\sum_{k=1}^{n}k^2\left[\sum_{j=k}^{\infty}(a_j^2+b_j^2)-\sum_{j=k+1}^{\infty}(a_j^2+b_j^2)\right]=\frac{1}{n^2}\sum_{k=1}^{n}k\sum_{j=k}^{\infty}(a_j^2+b_j^2)\leqq$$
$$\leqq\frac{1}{n}\sum_{k=1}^{n}\sum_{j=k}^{\infty}(a_j^2+b_j^2).$$

Schreiben wir einfachkeitshalber α_k statt $\sum_{j=k}^{\infty}(a_j^2+b_j^2)$, so folgt demnach

$$\frac{1}{4\pi}\int_0^{2\pi}[f(x+h)-f(x-h)]^2\,dx \leqq \alpha_n+\frac{1}{n}\sum_{k=1}^{n}\alpha_k.$$

Da aber $\{\alpha_n\}$ eine monoton abnehmende positive Zahlenfolge ist, kann das n-te Glied α_n nicht größer sein als das n-te arithmetische Mittel $\frac{1}{n}\sum_{k=1}^{n}\alpha_k$ der n ersten Glieder und daher ist

$$\int_0^{2\pi}[f(x+h)-f(x-h)]^2\,dx \leqq \frac{8\pi}{n}\sum_{k=1}^{n}\alpha_k. \tag{8}$$

Wir definieren nun die Funktion $\lambda(x)$ wie folgt:

$$\frac{1}{\lambda(x)}=\frac{1}{n}\sum_{k=1}^{n}\alpha_k \qquad (n\leqq x<n+1).$$

Dann gilt wegen $n\leqq\frac{1}{h}<n+1$ einerseits

$$\frac{1}{\lambda(1/h)}=\frac{1}{\lambda(n)},$$

anderseits ist $\lambda(x)$ eine monoton zunehmende Funktion, da $\frac{1}{\lambda(x)}$ als arithmetisches Mittel einer monotonen Nullfolge monoton abnehmend ist. Aus (8) ergibt sich somit

$$[\omega_2(\delta,f)]^2\leqq\sup_{0<h\leqq\delta}\int_0^{2\pi}[f(x+h)-f(x-h)]^2\,dx\leqq\sup_{0<h\leqq\delta}\frac{8\pi}{\lambda(1/h)}=O\left(\frac{1}{\lambda(1/\delta)}\right),$$

womit (4) bewiesen ist. Es bleibt noch zu zeigen, daß aus der angenommenen

Gültigkeit von (2) die Beziehung (3) folgt. Beachten wir zunächst, daß $\sum_{k=1}^{m} \alpha_k = o(m)$ ist, so ergibt sich aus der Definition von $\lambda(x)$ durch eine Abel-Transformation die Abschätzung

$$\int_{1}^{\infty} \frac{dx}{x\lambda(x)} \leq \sum_{n=1}^{\infty} \frac{1}{n^2} \sum_{k=1}^{n} \alpha_k = O(1) \sum_{n=1}^{\infty} \frac{\alpha_n}{n}.$$

Da aber nach Annahme die Beziehung (2) besteht, folgt (ebenfalls durch eine Abel-Transformation):

$$\sum_{n=1}^{\infty} \frac{\alpha_n}{n} = O(1) \sum_{n=1}^{\infty} (a_n^2 + b_n^2) \log n < \infty,$$

also

$$\int_{1}^{\infty} \frac{dx}{x\lambda(x)} < \infty,$$

d. h. die Bedingung (4) ist erfüllt und damit haben wir den Beweis unserer Behauptung zu Ende geführt.

Beweis des Satzes 2

Wählen wir die Zahlen α, β derart, daß $a \leq \alpha < \beta \leq b$ ist und für $0 < h \leq \delta$ die Abschätzungen

$$\int_{\alpha}^{\alpha+h} [f(t)]^2\, dt = O(h), \quad \int_{\beta}^{\beta+h} [f(t)]^2\, dt = O(h) \tag{9}$$

bestehen. Diese Beziehungen sind in allen Punkten α und β erfüllt, in welchen $[f(t)]^2$ die Ableitung ihres Integrals ist, d. h. in (a, b) fast überall. Man kann also α und β an a und b so nahe wählen, daß sich die Länge des Intervalls (α, β) von der Länge des Intervalls (a, b) um beliebig wenig unterscheidet. Wir setzen dann

$$g(x) = \begin{cases} f(x), & x \in (\alpha, \beta), \\ 0, & x \notin (\alpha, \beta). \end{cases}$$

Wir wollen den Betrag des Integrals

$$I(h) = \int_{0}^{2\pi} [g(x+h) - g(x)]^2\, dx$$

durch die Zerlegung

$$I(h) = \int_{0}^{\alpha-h} + \int_{\alpha-h}^{\alpha} + \int_{\alpha}^{\beta-h} + \int_{\beta-h}^{\beta} + \int_{\beta}^{2\pi}$$

abschätzen. Zunächst ist

$$\int_0^{\alpha-h}[g(x+h)-g(x)]^2dx=0,\quad \int_\beta^{2\pi}[g(x+h)-g(x)]^2\,dx=0,$$

da in diesen Intervallen $g(x+h)\equiv g(x)$ ist. In $(\alpha-h,\alpha)$ ist aber $g(x)=0$, also nach (9)

$$\int_{\alpha-h}^{\alpha}[g(x+h)-g(x)]^2dx=\int_{\alpha-h}^{\alpha}[g(x+h)]^2\,dx=\int_{\alpha}^{\alpha+h}[f(t)]^2\,dt=O(h).$$

Auf derselben Weise ergibt sich

$$\int_{\beta-h}^{\beta}[g(x+h)-g(x)]^2\,dx=O(h)$$

und endlich gilt

$$\int_{\alpha}^{\beta-h}[g(x+h)-g(x)]^2\,dx=\int_{\alpha}^{\beta-h}[f(x+h)-f(x)]^2\,dx=O\left(\frac{1}{\lambda(1/\delta)}\right).$$

Addiert man diese Ungleichungen, so folgt

$$I(h)=O\left(\frac{1}{\lambda(1/\delta)}\right)+O(h).$$

Es ist aber keine Beschränkung der Allgemeinheit, wenn wir $\lambda(x)\leqq x$, also

$$\frac{1}{\lambda(1/h)}\geqq h$$

annehmen, woraus man wegen der Monotonität von $\lambda(x)$

$$I(h)=O\left(\frac{1}{\lambda(1/\delta)}\right)$$

erhält. Ähnlich läßt sich auch der Fall $-\delta\leqq h<0$ behandeln. Wir erhalten somit die Abschätzung

$$\omega_2(g,\delta)=\sup_{|h|\leqq\delta}I(h)=O\left(\frac{1}{\lambda(1/\delta)}\right).$$

Die Funktion $g(x)$ erfüllt daher die Bedingungen des Satzes 1, folglich konvergiert die Fourierreihe von $g(x)$ fast überall. Da aber in (α,β) die Funktion $f(x)$ mit $g(x)$ übereinstimmt, sind nach dem Lokalisationssatz die Fourierreihen der beiden Funktionen in (α,β) äquikonvergent. Die Reihe (1) konvergiert also in (α,β) fast überall und da sich die Länge des Intervalls (α,β) von der Länge des Intervalls (a,b) um beliebig wenig unterscheidet, ist (1) auch in (a,b) fast überall konvergent, w. z. b. w.

(Eingegangen am 19. Mai 1953.)

ВЛИЯНИЕ СТРУКТУРНЫХ СВОЙСТВ ФУНКЦИИ НА СХОДИМОСТЬ ЕЁ РЯДА ФУРЬЕ ПОЧТИ ВСЮДУ

Г. АЛЕКСИЧ (Будапешт)

(Резюме)

Пусть $f \in L^2$ и исследуем сходимость почти всюду ряда Фурье

(1) $$f(x) \sim \frac{a_0}{2} + \sum_{n=1}^{\infty} (a_n \cos nx + b_n \sin nx).$$

Рассмотрим для этой цели выражение

$$\omega_2(\delta, f) = \sup_{|h| \leqq \delta} \left\{ \int_0^{2\pi} [f(x+h) - f(x)]^2 \, dx \right\}^{1/2},$$

дающсе некоторое представление о структуре функции $f(x)$. Пусть $\lambda(x) > 0$ — монотонно возрастающая функция, удовлетворяющая условию

(2) $$\int_1^{\infty} \frac{dx}{x\lambda(x)} < \infty.$$

Доказываем следующие теоремы:

1. Для выполнения условия Колмогорова—Селиверстова—Плесснера

$$\sum_{n=1}^{\infty} (a_n^2 + b_n^2) \ln n < \infty$$

необходимо и достаточно существование функции $\lambda(x)$, удовлетворяющей условию (2) и такой, что

$$\omega_2(\delta, f) = O\left(\frac{1}{\sqrt{\lambda(1/\delta)}}\right).$$

2. Если на интервале $(a, b) \subset (0, 2\pi)$ $f \in L^2$ и выполняется условие

$$\sup_{|h| < \delta} \left\{ \int_a^b [f(x+h) - f(x)]^2 \, dx \right\}^{1/2} = O\left(\frac{1}{\lambda(1/\delta)}\right),$$

где $\lambda(x)$ удовлетворяет условию (2), то ряд Фурье (1) сходится почти всюду на интервале (a, b).

KREISAUSFÜLLUNGEN DER HYPERBOLISCHEN EBENE

Von

L. FEJES TÓTH (Veszprém)

(*Vorgelegt von* G. HAJÓS)

Bekanntlich[1] ist die (später zu definierende) Lagerungsdichte d eines unendlichen Systems von in der euklidischen Ebene ausgestreuten, nicht übereinandergreifenden kongruenten Kreisen

$$d \leqq \frac{\pi}{\sqrt{12}} = 0{,}906\ldots.$$

Kurz gefaßt: es läßt sich höchstens 90,6...% der euklidischen Ebene durch gleichgroße Kreise ausfüllen. Diese Schranke wird durch diejenige Lagerung erreicht, bei welcher jeder Kreis von 6 anderen berührt wird.

In diesem Aufsatz wenden wir uns dem analogen Problem in der hyperbolischen Ebene zu. Wir zeigen, daß hier

$$d \leqq \frac{3}{\pi} = 0{,}955\ldots \tag{1}$$

gilt und daß die rechtsstehende Schranke sich durch keine kleinere ersetzen läßt. Wir werden die Abschätzung (1) als Korollar einer allgemeineren Ungleichung erhalten, die auch gewisse frühere, bezüglich der Kreisausfüllungen der Kugel erzielte Resultate umfaßt.

Unter einer Kugel der Krümmung k wird für $k > 0$ eine gewöhnliche Kugelfläche vom Radius $1/\sqrt{k}$, für $k = 0$ die euklidische Ebene und für $k < 0$ eine hyperbolische Ebene vom Parameter $\sqrt{-k}$ verstanden. Die erwähnte Ungleichung lautet dann:

Sind auf einer Kugel der Krümmung k wenigstens drei[2] *Kreise vom Radius r eingelagert, so ist ihre Lagerungsdichte*

$$d \leqq D(a) = \frac{3\operatorname{cosec}\frac{\pi}{a} - 6}{a-6}; \quad D(6) = \lim_{a\to 6} D(a) = \frac{\pi}{\sqrt{12}}, \tag{2}$$

[1] Vgl. die zusammenfassende Darstellung des Verf.: *Lagerungen in der Ebene, auf der Kugel und im Raum* (Berlin-Göttingen-Heidelberg, 1953).

[2] Diese Einschränkung ist im Falle $k \leqq 0$ nicht nötig, da es sich hier stets um unendlich viele Kreise handeln muß, um positive Lagerungsdichte zu erreichen.

wobei a durch

$$\operatorname{cosec}\frac{\pi}{a} = 2\cos\sqrt{k}\,r$$

definiert wird.[3]

Wir erklären die Dichte eines Bereichsystems $\{S_i\}$ in einem Bereich B durch den Quotient[4] $\Sigma BS_i/B$, wo BS_i den Inhalt des Durchschnittes von B und S_i bedeutet. Dann ist $D(a)$ die Dichte von drei einander gegenseitig berührenden Kreisen vom Radius r einer Kugel der Krümmung k im Dreieck ihrer Zentralen. $2\pi/a$ bedeutet einen Winkel dieses Dreiecks, sodaß sich a als die „Anzahl" derjenigen Kreise interpretieren läßt, die sich an einem Kreis anlegen lassen (Abb. 1). Während in der euklidischen Ebene $a=6$ ist, haben wir auf der gewöhnlichen Kugel $a<6$ und in der hyperbolischen Ebene $a>6$.

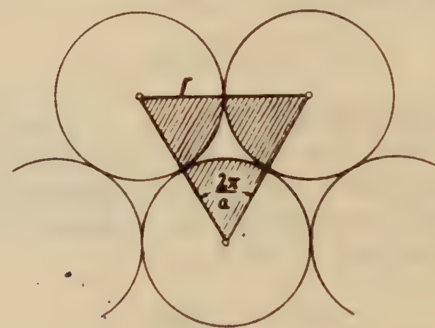


Abb. 1

Die Ungleichung (2) ist für jeden ganzzahligen Wert von $a \geqq 2$ genau.[5] Gleichheit wird durch diejenigen Kreissysteme erreicht, in denen jeder Kreis durch genau a weitere berührt wird. Die Existenz eines derartigen Kreissystems folgt aus der bemerkenswerten Tatsache,[6] daß es zu jedem ganzzahligen Zahlenpaar p, q mit $p \geqq 2$, $q \geqq 2$ ein reguläres Netz existiert, das den drei Fällen $\frac{1}{p}+\frac{1}{q} \gtreqless \frac{1}{2}$ entsprechend entweder die gewöhnliche Kugel,

[3] Für $k>0$ folgt aus der Bedingung, daß die Anzahl der Kreise $\geqq 3$ ist, daß $\sqrt{k}\,r \leqq \pi/3$, d. h. $2\cos\sqrt{k}\,r \geqq 1$ ausfällt. Ist $k<0$, so tritt natürlich in der Definition von a die hyperbolische Cosinusfunktion auf.

[4] Im Folgenden bezeichnen wir einen Bereich und seinen Flächeninhalt mit demselben Symbol.

[5] Für nicht ganzzahlige Werte von a wurde die maximale Lagerungsdichte von K. Schütte und B. L. van der Waerden [Auf welcher Kugel haben 5, 6, 7, 8 oder 9 Punkte mit Mindestabstand Eins Platz? *Math. Annalen,* **123** (1951), S. 96—124] für $a \leqq 2\pi/\operatorname{arc}\cos 0{,}25 \doteq 4{,}7668\ldots$ bestimmt.

[6] Vgl. z. B. D. M. Y. Sommerville, The regular divisions of space of n dimensions and their metrical constants. Rendiconti circ. mat. Palermo, **48** (1924), 9—22.

oder die euklidische Ebene, oder die hyperbolische so in reguläre p-Ecke zerlegt, daß bei jeder Ecke q Kanten zusammenkommen. Wir bezeichnen ein solches Netz nach L. SCHLÄFLI mit $\{p, q\}$. Die in unserem Schema einge-

{2,2}	{2,3}	{2,4}	{2,5}	{2,6}	{2,7}	···
{3,2}	{3,3}	{3,4}	{3,5}	{3,6}	{3,7}	···
{4,2}	{4,3}	{4,4}	{4,5}	{4,6}	{4,7}	···
{5,2}	{5,3}	{5,4}	{5,5}	{5,6}	{5,7}	···
{6,2}	{6,3}	{6,4}	{6,5}	{6,6}	{6,7}	···
{7,2}	{7,3}	{7,4}	{7,5}	{7,6}	{7,7}	···
.	.	.	.	.	.	...
.	.	.	.	.	.	...
.	.	.	..	.	.	...

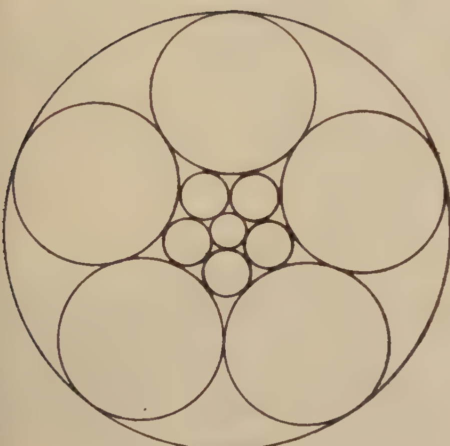


Abb. 2

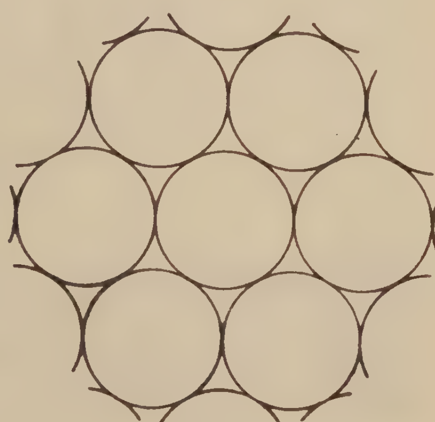


Abb. 3

zeichneten Linien trennen voneinander diejenigen Netze, die sich auf einer Kugel von positiver, verschwindender bzw. negativer Krümmung realisieren lassen. Bei einem ganzzahligen Wert von a wird die dichteste Kreislagerung durch die Flächeninkreise eines $\{a, 3\}$ repräsentiert. Diese Inkreise liefern nämlich als Lagerungsdichte die in (2) angegebene obere Schranke. Hier sind die Kreismittelpunkte Ecken eines dualen Netzes $\{3, a\}$.

Wir haben in den Abbildungen 2, 3 und 4 die dichtesten Kreislagerungen für $a = 5$, 6 bzw. 7 dargestellt. Die Abbildung 2 ($a = 5$) ist eine stereographische Projektion von 12 ikosaedrisch angeordneten Kreisen. Der Fall $a = 7$ (Abb. 4) ist im Poincaréschen Modell dargestellt.

Die in Abb. 5 dargestellte Funktion $D(a)$ strebt für $a \to \infty$ ständig zunehmend dem Grenzwert $3 : \pi$ zu, sodaß sie im Einklang mit (1) unterhalb diesem Grenzwert bleibt. Bemerken wir jedoch, daß indem zur Ausfüllung

der hyperbolischen Ebene auch Grenzkreise (Horozyklen) zugelassen werden, in (1) auch Gleichheit erreicht werden kann. Abb. 6 stellt die „absolut“ dichteste Kreislagerung auf Flächen konstanter Krümmung dar, d. h. diejenige Anordnung von (wenigstens drei) kongruenten „Kreisen“, deren Lagerungsdichte unabhängig von der Flächenkrümmung und der Größe der Kreise den größtmöglichen Wert erreicht. Hier sind die „Kreismittelpunkte“ Ecken des

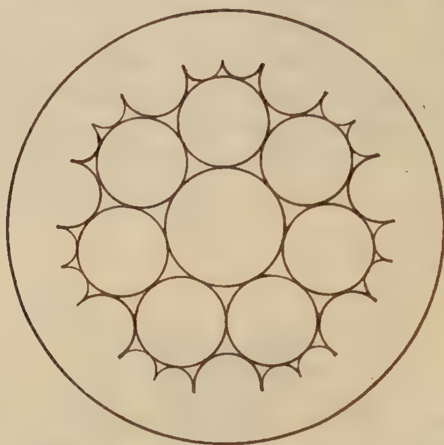


Abb. 4.

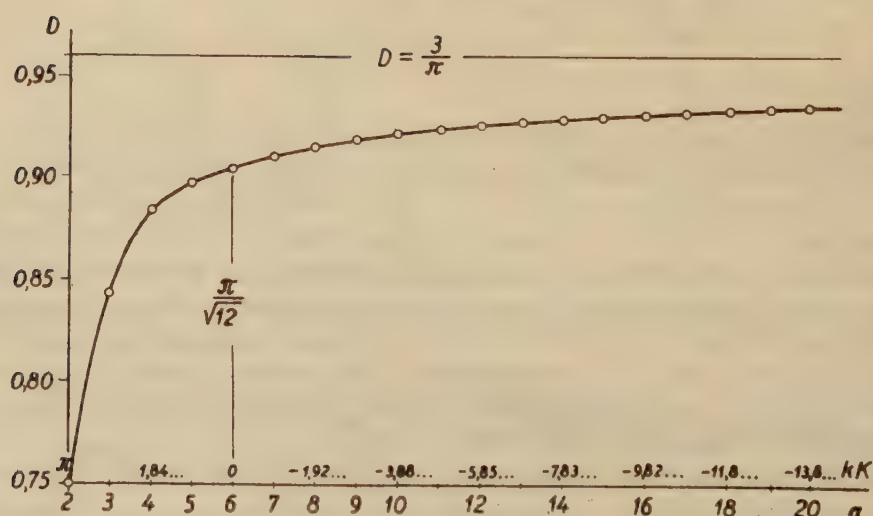


Abb. 5

aus der Theorie der Modulfunktionen wohlbekannten Netzes $\{3, \infty\}$. Die betreffende maximale Lagerungsdichte beträgt $3/\pi$, was zu einer recht interessanten Interpretation der Zahl π Anlaß gibt.

Für $k > 0$ definieren wir die Lagerungsdichte als die Inhaltssumme der Kreise geteilt durch den Flächeninhalt der Kugel. In der euklidischen Ebene schlagen wir um einen festen Punkt O einen Kreis $K(R)$ vom Halbmesser R und bezeichnen die Inhaltssumme der ganz zu $K(R)$ gehörigen Kreise mit $T(R)$. Dann definieren wir d durch

$$d = \overline{\lim_{R \to \infty}} \frac{T(R)}{K(R)}.$$

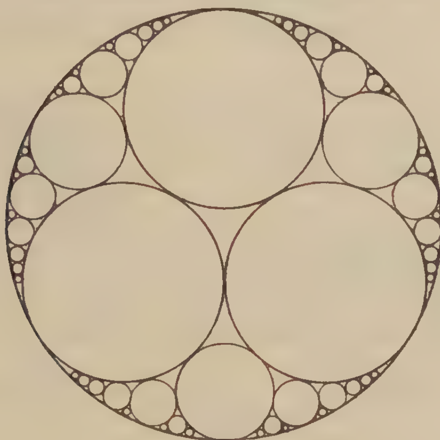


Abb. 6

Es läßt sich leicht zeigen, daß d nicht von der Wahl des Ursprungspunktes O abhängt. Ferner gelangen wir zu demselben Wert d, wenn wir $T(R)$ durch die Inhaltssumme derjenigen Kreise ersetzen, die gemeinsame Punkte mit $K(R)$ aufweisen. Folglich läßt sich d auch als Grenzwert der Dichte der Kreise in $K(R)$ erklären. All dies folgt aus der Tatsache, daß

$$\frac{K(R+c)-K(R)}{K(R)} = \frac{2Rc+c^2}{R^2}$$

bei festem c für $R \to \infty$ gegen Null strebt.

In der hyperbolischen Ebene trifft dies aber wegen

$$K(R) = \frac{2\pi}{k}(1-\cos\sqrt{k}R) = \frac{2\pi}{\varkappa^2}(\operatorname{ch}\varkappa R - 1); \quad k = -\varkappa^2$$

nicht zu, sodaß hier die Erklärung der Lagerungsdichte größere Behutsamkeit erfordert. Wir werden aber die mit der Dichtendefinition verbundenen Schwierigkeiten in einfacher Weise umgehen, indem wir zeigen werden, daß sich unsere Kugel (von beliebiger reeller Krümmung) so in Dreiecke zerlegen läßt, daß die Dichte in jedem Dreieck höchstens $D(a)$ ist. Das bedeutet, daß die Ungleichung (2) bei einer jeden „vernünftigen" Definition von d bestehen muß. Jedenfalls gilt (2), wenn d als irgendein Mittelwert der Dichten in den von uns zu konstruierenden Dreiecken definiert wird.

Wir nennen ein System von kongruenten Kreisen gesättigt, wenn jeder zu den Kreisen unseres Systems kongruente Kreis der Kugel gemeinsame innere Punkte mit wenigstens einem Kreis des Systems aufweist. Ist unser Kreissystem nicht gesättigt, so kann es durch Hinzufügung weiterer Kreise gesättigt werden. Durch nachträgliche Fortschaffung dieser Kreise nimmt die Dichte in keinem Dreieck zu, sodaß wir uns von vornherein auf gesättigte Systeme beschränken dürfen. Um Fallunterscheidungen zu vermeiden, beschränken wir uns ferner auf den Fall[7] $16kr^2 \leq \pi^2$. Dann liegen die Mittelpunkte $O_1, O_2, \ldots$ der Kreise $K_1, K_2, \ldots$ nicht auf einer Halbkugel, da sonst $\{K_i\}$ nicht gesättigt wäre.

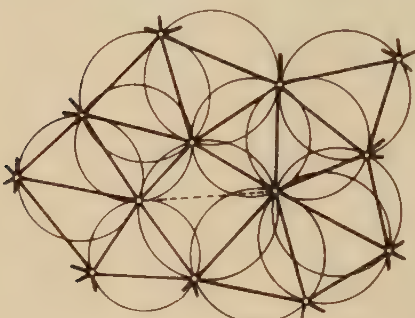


Abb. 7

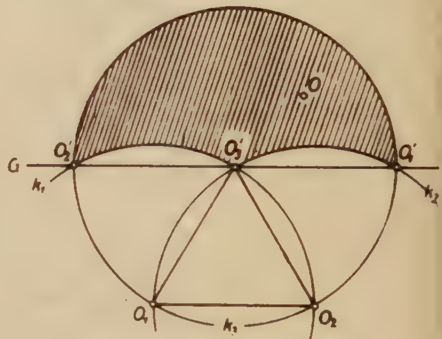


Abb. 8

Wir betrachten einen Kreis $\mathfrak{K}$ von der Eigenschaft, daß wenigstens drei Punkte von $\{O_i\}$ auf den Rand von $\mathfrak{K}$ fallen, ohne daß $\mathfrak{K}$ Punkte von $\{O_i\}$ im Inneren enthält (Abb. 7). Ein solcher Kreis ist sicher vorhanden. Man sieht sogar leicht ein, daß die Gesamtheit $\{\mathfrak{K}\}$ der Kreise von dieser Eigenschaft die Kugel überdeckt. Der Halbmesser eines jeden Kreises $\mathfrak{K}$ ist $< 2r$, da sonst der konzentrische Kreis vom Radius r keinen gemeinsamen inneren Punkt mit den Kreisen $K_1, K_2, \ldots$ hätte, d. h. $\{K_i\}$ nicht gesättigt wäre. Die am Rand von $\mathfrak{K}$ liegenden Punkte des Systems $\{O_i\}$ bestimmen ein $\mathfrak{K}$ einbeschriebenes Polygon $\mathfrak{P}$. Wir zeigen, daß die Gesamtheit $\{\mathfrak{P}\}$ dieser Polygone die Kugel schlicht und lückenlos bedeckt.[8]

Wir zeigen zunächst, daß zwei Polygone $\mathfrak{P}$ und $\mathfrak{P}'$ von $\{\mathfrak{P}\}$ nicht übereinandergreifen. Da die Umkreise $\mathfrak{K}$ und $\mathfrak{K}'$ der Polygone nach Definition nicht einander enthalten können, haben wir nur den Fall zu untersuchen, daß $\mathfrak{K}$ und $\mathfrak{K}'$ einander in zwei Punkten, sagen wir in P und Q durchsetzen. Da aber mit eventueller Ausnahme der Punkte P und Q keine Ecke von $\mathfrak{P}$ oder $\mathfrak{P}'$ dem Durchschnitt $\mathfrak{K}\mathfrak{K}'$ angehört, wird $\mathfrak{P}$ und $\mathfrak{P}'$ durch PQ getrennt.

[7] Die Ungleichung $16kr^2 > \pi^2$ besteht nur in dem leicht zu behandelnden Fall von drei oder vier Kreisen.

[8] Im Falle $k > 0$ stimmt $\{\mathfrak{P}\}$ mit dem sphärischen Netz der konvexen Hülle der Kreismittelpunkte überein.

Wenn nicht die ganze Kugel durch $\{\mathfrak{P}\}$ bedeckt wäre, so gäbe es entweder ein Polygon $\mathfrak{P}$, an dessen einer Seite sich kein Polygon von $\{\mathfrak{P}\}$ anschließt, oder gäbe es einen Punkt P, der ein Häufungspunkt von Polygonen $\mathfrak{P}_1, \mathfrak{P}_2, \ldots$ mit Eckpunkten $O_1, O_2, \ldots$ ist. Die erste Möglichkeit kann nicht auftreten, worauf leicht aus der Definition der Polygone $\mathfrak{P}$ gefolgert werden kann. Die zweite Möglichkeit erweist sich ebenfalls als unmöglich, da dann der um P geschlagene Kreis vom Halbmesser $2r$ unendlich viele Punkte der Folge $O_1, O_2, \ldots$ enthalten möchte, was nicht auftreten kann, da jeder Abstand $O_i O_j \geqq 2r$ ist. Damit ist gezeigt, daß $\{\mathfrak{P}\}$ zugleich die Kugel überdeckt.

Zerlegen wir die mehr als dreieckigen Polygone irgendwie durch Diagonale in Dreiecke, so haben wir ein auf $\{O_i\}$ aufgespanntes Dreiecksnetz vor uns. Wir haben zu zeigen, daß die Dichte des Kreissystems $\{K_i\}$ in jedem Dreieck $\leqq D(a)$ ist.

Es sei $\Delta \equiv O_1 O_2 O_3$ ein Dreieck unseres Netzes. Wir werden später zeigen, daß keiner der Kreise K_1, K_2, K_3 die gegenüberliegende Dreiecksseite treffen kann. Es folgt daraus, daß in Δ außer den Kreisen K_1, K_2, K_3 kein weiterer Kreis des Systems $\{K_i\}$ hineindringen kann. Somit ist die Dichte des Kreissystems in Δ

$$\frac{\sigma}{2\pi} K : \Delta,$$

wo σ die Winkelsumme von Δ und K den Inhalt eines Kreises bedeutet. Wir haben aber mit Rücksicht auf $k\Delta = \sigma - \pi$

$$\frac{\sigma}{2\pi} K : \Delta = \frac{K}{2\pi}\left(k + \frac{\pi}{\Delta}\right).$$

Es handelt sich also um die Bestimmung des Minimums von Δ unter den Bedingungen, daß jede Seite von $\Delta \geqq 2r$ und der Umkreisradius $< 2r$ ausfällt.

Es sei $O_1 O_2 = \varrho$ die kürzeste Seite von Δ und $\Delta' \equiv O_1 O_2 O_3'$ ein gleichseitiges Dreieck, das an der mit O_3 übereinstimmenden Seite von $O_1 O_2$ liegt (Abb. 8). Wir schlagen um jede Ecke dieses Dreiecks je einen Kreis k_1, k_2, k_3 vom Radius ϱ. Dann liegt O_3 außerhalb oder am Rand der Kreise k_1, k_2. Andererseits liegt O_3 innerhalb k_3, da sonst der Umkreisradius von $\Delta \geqq 2r$ wäre.

Wir betrachten den Ort G derjenigen Punkte, die mit O_1 und O_2 ein mit Δ' flächengleiches Dreieck bestimmen. Es seien O_1' und O_2' die von O_1 und O_2 verschiedenen Schnittpunkte von k_2 und k_3 bzw. k_1 und k_3. Da $O_1 O_2 O_1' O_3'$ ein Rhombus ist, sind die Dreiecke $O_1 O_2 O_1'$ und $O_1 O_2 O_3'$ flächengleich. Folglich gehört O_1' und — aus selben Gründen — auch O_2' zu G. Bekanntlich ist G den Fällen $k \gtreqless 0$ entsprechend ein Kreisbogen (Lexellscher Kreis), eine Gerade bzw. ein Hyperzyklus,[9] nämlich die durch O_3' hindurchgehende Abstandslinie derjenigen Geraden, welche die Mittelpunkte der Seiten

$O_3'O_1$ und $O_3'O_2$ verbindet. Bedenken wir noch, daß G außer den Punkten O_1', O_3', O_2' keine weiteren Punkte mit k_2 bzw. k_1 gemein hat, so schließt man leicht, daß O_3 nicht „unterhalb" G liegen kann. Folglich ist $\Delta \geqq \Delta'$ und Gleichheit gilt nur, wenn O_3 in den Punkt O_3' fällt. Wir haben daher a fortiori

$$\Delta \geqq \bar{\Delta} = \frac{\pi}{ka}(6-a),$$

wobei $\bar{\Delta}$ den Inhalt eines gleichseitigen Dreiecks der Seitenlänge $2r$ bedeutet. Mithin gilt die zu beweisende Ungleichung

$$\frac{\sigma}{2\pi}K:\Delta \leqq \frac{K}{2\pi}\left(k+\frac{\pi}{\bar{\Delta}}\right)=D(a).$$

Wir haben noch zu zeigen, daß die Kreise K_1, K_2, K_3 keinen gemeinsamen Punkt mit der gegenüberliegenden Seite von Δ haben können. Wir zeigen, daß dasselbe sogar für die konzentrischen Kreise U_1, U_2, U_3 vom Halbmesser $\frac{\varrho}{2} \geqq r$ gilt. U_3 besitzt keine gemeinsamen inneren Punkte mit U_1 und U_2, da sonst $O_1O_2 = \varrho$ nicht die kürzeste Seite von Δ wäre. Da ferner U_1 und U_2 die Seite O_1O_2 zusammen überdecken, kann U_3 diese Seite nicht treffen. Bewegt sich nun O_3 in den von k_1, k_2, k_3 begrenzten oben betrachteten Kreisbogendreieck, so berührt O_1O_3 und O_2O_3 den Kreis U_2 bzw. U_1 nur in den Lagen $O_3 \equiv O_1'$ bzw. $O_3 \equiv O_2'$. Da aber O_3 im Inneren von k_3 liegt, sind diese Lagen ausgeschlossen. Somit kann U_1 und U_2 die Strecken O_2O_3 bzw. O_1O_3 weder schneiden, noch berühren.

Damit ist der Beweis beendet.

(Eingegangen am 30. Januar 1953.)

[9] Diese Tatsache war schon J. Bolyai bekannt. (*Appendix* §§ 39 und 41.)

ЗАПОЛНЕНИЕ ГИПЕРБОЛИЧЕСКОЙ ПЛОСКОСТИ КРУГАМИ

Л. ФЕЕШ ТОТ (Веспрем)

(Резюме)

Автор даёт неравенство для плотности одинаковых непересекающихся кругов расположенных на шаре, эвклидовой или гиперболической плоскости, откуда следует что эта плотность во всех случаях $\leqq \frac{3}{\pi}$. Равенство достигается для орициклов, подходяще расположенных на гиперболической плоскости.

KREISÜBERDECKUNGEN DER HYPERBOLISCHEN EBENE

Von

L. FEJES TÓTH (Veszprém)

(*Vorgelegt von* G. Hajós)

In einer vorigen Arbeit[1] habe ich das Problem der dichtesten Kreislagerung auf Flächen konstanter Krümmung behandelt. Der vorliegende Aufsatz ist dem dualen Problem, nämlich dem Problem der dünnsten Kreisüberdeckung gewidmet.

Bekanntlich[2] ist die Dichte[3] eines Systems von kongruenten, die euklidische Ebene vollständig überdeckenden Kreisen

$$D \geqq \frac{2\pi}{\sqrt{27}} = 1,209\ldots.$$

Gleichheit wird in demjenigen Fall erreicht, wenn jeder Kreis durch die übrigen in den Ecken eines regulären Sechsecks geschnitten wird. Wir werden zeigen, daß in der hyperbolischen Ebene

$$D \geqq \frac{\sqrt{12}}{\pi} = 1,1026\ldots \tag{1}$$

gilt.[4] Die rechtsstehende Schranke läßt sich durch keine größere ersetzen. Dieses Resultat wird sich als Korollar einer allgemeinen Ungleichung ergeben, die auch gewisse frühere, bezüglich der Kreisüberdeckungen der Kugel erhaltene Ergebnisse[5] umfaßt und bei deren Formulierung unter einer Kugel der Krümmung k dem Vorzeichen von k entsprechend entweder eine gewöhnliche Kugelfläche vom Radius $1/\sqrt{k}$, oder die euklidische Ebene, oder die hyperbolische Ebene vom Parameter $\sqrt{-k}$ verstanden wird.

[1] Kreisausfüllungen der hyperbolischen Ebene, *Acta Math. Acad. Sci. Hung.*, 4 (1953), S. 103—110.

[2] Vgl. L. Fejes Tóth, *Lagerungen in der Ebene, auf der Kugel und im Raum* (Berlin-Göttingen-Heidelberg, 1953).

[3] Vgl. die unter [1] angeführte Arbeit.

[4] Im Sonderfall, daß jeder Flächenteil höchstens zweifach bedeckt ist, fand diese Ungleichung kurz vorher J. Molnár.

[5] S. das unter [2] zitierte Werk.

Wird die Kugel der Krümmung k durch wenigstens drei kongruente Kreise vom Radius r überdeckt, so ist die Überdeckungsdichte

$$(2)\qquad D \geqq d(A) = \frac{\sqrt{12}\,\mathrm{ctg}\,\frac{\pi}{A} - 6}{A-6}\,; \quad d(6) = \lim_{A\to 6} d(A) = \frac{2\pi}{\sqrt{27}}\,,$$

wobei A durch

$$\mathrm{ctg}\,\frac{\pi}{A} = \sqrt{3}\,\cos\sqrt{k}\,r$$

definiert wird.

Schlagen wir um die Ecken eines regulären Dreiecks $\bar{\varDelta}$ vom Umkreisradius r je einen Kreis vom Radius r, so ist $d(A)$ nichts anderes als die Dichte dieser Kreise in $\bar{\varDelta}$ (Abb. 1). Ein Winkel von $\bar{\varDelta}$ beträgt $2\pi/A$, sodaß A sich als die „Anzahl" derjenigen mit $\bar{\varDelta}$ kongruenten Dreiecke interpretieren läßt, die sich um einen Punkt anlegen lassen. Es gilt den drei Fällen $k \gtreqless 0$ entsprechend $A \lesseqgtr 6$.

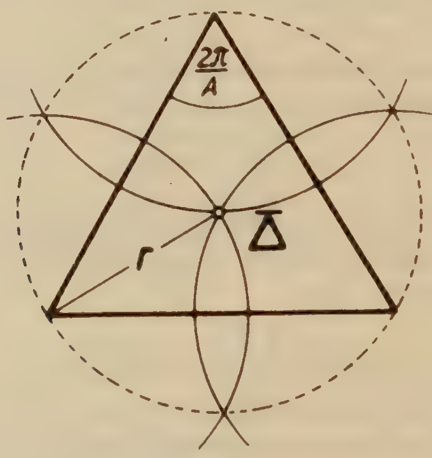


Abb. 1

Die Ungleichung (2) läßt sich für ganzzahlige Werte von $A \geqq 2$ nicht verbessern. Gleichheit besteht für das System der Flächenumkreise eines regulären Dreikantnetzes mit A-seitigen Flächen.

Es läßt sich zeigen, daß $d(A)$ mit wachsendem A ständig abnehmend dem Grenzwert $\sqrt{12}/\pi$ zustrebt (Abb. 2), sodaß D im Einklang mit (1) oberhalb dieses Grenzwertes bleibt. Werden aber zur Überdeckung auch Grenzkreise zugelassen, so kann in (1) auch Gleichheit zutreffen. Abb. 3 stellt die „absolut" dünnste Kreisüberdeckung der hyperbolischen Ebene im Poincaréschen Modell dar.

Wir können voraussetzen, daß die Kreismittelpunkte keinen Häufungspunkt besitzen, da sonst dem Kreissystem eine unendliche Dichte zuge-

schrieben werden könnte. Wir betrachten dasjenige, auf die Kreismittelpunkte aufgespannte Dreiecksnetz, das dadurch charakterisiert ist, daß die Dreiecksumkreise keine Ecken des Netzes in ihrem Inneren enthalten[6] (Abb. 4).

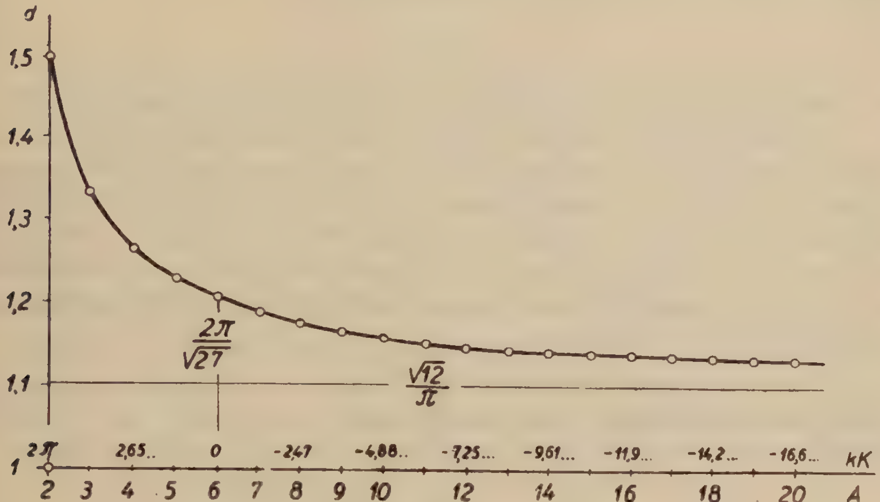


Abb. 2

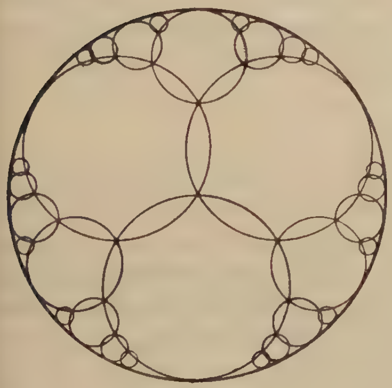


Abb. 3

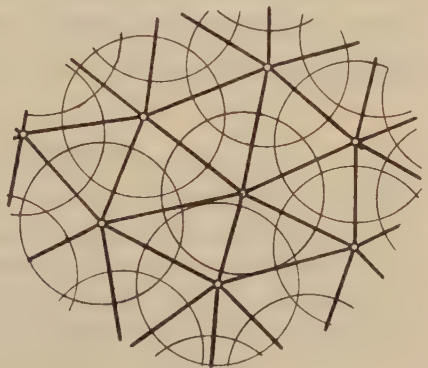


Abb. 4

Jeder Kreis wird durch die von seinem Mittelpunkt ausstrahlenden Kanten dieses Netzes in Kreisausschnitte zerlegt. Wir wollen bei der Berechnung der Dichte in einem Dreieck Δ die durch die Dreiecksseiten bestimmten drei Kreisausschnitte auch dann bei Δ in Betracht nehmen, wenn diese aus Δ herausragen. Wir denken also die eventuell herausragenden Kreisteile vom Kreis abgeschnitten und auf Δ gelegt. Nach einer anderen, mit der vorigen

[6] S. den unter [1] zitierten Aufsatz.

gleichbedeutenden Vorstellung können wir uns die „Massen" der Kreise auf konzentrische Kreisscheiben konzentriert denken, die in der Vereinigungsmenge der im betreffenden Kreismittelpunkt zusammentreffenden Dreiecke liegen. Dann ist die Dichte des Kreissystems in Δ

$$\frac{\sigma}{2\pi} K : \Delta,$$

wo σ die Winkelsumme von Δ und K den Inhalt eines Kreises bedeutet.[7]

Wir machen jetzt von der definierenden Eigenschaft des Netzes Gebrauch, nach der kein Kreismittelpunkt im Inneren des Umkreises von Δ liegt. Da andererseits der Umkreismittelpunkt sicher in einem Kreis unseres Systems enthalten ist, so läßt sich schließen, daß der Umkreisradius von Δ nie größer als r sein kann. Folglich gilt (nach einer wohlbekannten, in der sphärischen, euklidischen und hyperbolischen Geometrie gleichfalls gültigen Maximaleigenschaft des regulären Dreiecks)

$$\Delta \leqq \bar{\Delta}.$$

Wir haben daher mit Rücksicht auf $k\Delta = \sigma - \pi$

$$\frac{\sigma}{2\pi} K : \Delta = \frac{K}{2\pi}\left(k + \frac{\pi}{\Delta}\right) \geqq \frac{K}{2\pi}\left(k + \frac{\pi}{\bar{\Delta}}\right) = d(A).$$

Damit ist gezeigt, daß die Dichte des Kreissystems mit der obigen Vereinbarung in jedem Dreieck $\geqq d(A)$ ist.[8] Dasselbe gilt dann auch für die Überdeckungsdichte bezüglich der ganzen Kugel, wenn diese als irgendein Mittelwert der Dichten $\frac{\sigma}{2\pi} K : \Delta$ definiert wird.

(Eingegangen am 16. März 1953.)

[7] Δ und $\bar{\Delta}$ bezeichnen zugleich die Inhalte der Dreiecke.

[8] Diese Ungleichung gilt wahrscheinlich auch dann, wenn bei der Berechnung der Dichte in Δ nur die tatsächlich in Δ enthaltenen Kreisteile berücksichtigt werden. Jedenfalls läßt sich durch unsere Vereinbarung der Beweis dieser Vermutung ersparen.

ПОКРЫТИЕ ГИПЕРБОЛИЧЕСКОЙ ПЛОСКОСТИ КРУГАМИ

Л. ФЕЕШ ТОТ (Веспрем)

(Резюме)

Автор даёт неравенство для плотности одинаковых кругов, покрывающих шар, эвклидовую или гиперболическую плоскость, откуда следует, что эта плотность во всех случаях $\geqq \frac{\sqrt{12}}{\pi}$. Равенство достигается для покрывающих гиперболическую плоскость орициклов, расположенных в определённом порядке.

VERSCHÄRFUNG EINES HARDY—LITTLEWOODSCHEN SATZES

Von
P. SZÜSZ (Budapest)
(*Vorgelegt von* P. TURÁN)

In der vorliegenden Note beweisen wir den folgenden

SATZ. *Es sei ω irrational, k eine natürliche Zahl und $\{n^k\omega\} = n^k\omega - [n^k\omega]$. Bedeuten dann $\alpha_1, \alpha_2, \ldots, \alpha_k$ beliebige Zahlen mit $0 \leqq \alpha_\varkappa < 1$ $(\varkappa = 1, 2, \ldots, k)$ und ist $\varepsilon > 0$ gegeben, so gibt es eine nur von ε, k und ω abhängige Zahl m so, daß bei beliebigem ν für mindestens ein ganzes n mit $\nu \leqq n \leqq \nu + m$ die Relationen:*

$$|\{n^\varkappa\omega\} - \alpha_\varkappa| < \varepsilon \qquad (\varkappa = 1, 2, \ldots, k)$$

stattfinden.

Dieser Satz ist eine Verschärfung eines Satzes von HARDY—LITTLEWOOD [1]. Der Satz von HARDY—LITTLEWOOD besagt, daß bei beliebig gegebenem $\varepsilon > 0$ die Relationen

$$|\{n^\varkappa\omega\} - \alpha_\varkappa| < \varepsilon \qquad (\varkappa = 1, 2, \ldots, k)$$

mit geeignetem ganzen n erfüllt werden können. Ich benützte den obigen Satz als Hilfssatz zu einem elementaren (d. h. ohne Benützung von Weylschen trigonometrischen Summen arbeitenden) Beweis für die bekannte Tatsache, daß die Zahlen $\{n^k\omega\}$ in $(0, 1)$ gleichverteilt liegen. Meinen Beweis veröffentlichte ich nicht, weil, wie ich dies bereits nach der Ausarbeitung meines Beweises erfuhr, V. BERGSTRÖM [2], [3] bereits im Jahre 1935 einen im Grundgedanken ähnlichen, wenn auch in der Durchführung der Rechnung abweichenden Beweis mitgeteilt hat.

BEWEIS. Der Beweis geschieht durch vollständige Induktion nach k. Es seien ω und ε gegeben. Unser Satz ist für $k = 1$ gültig. Die Multipla von ω liegen nämlich mod 1 überall dicht. Wir wählen ein natürliches a mit $\{a\omega\} = \varepsilon_a < \varepsilon$ und betrachten im folgenden nur die Zahlen $\{na\omega\} = \{n\varepsilon_a\}$ $(n = 1, 2, \ldots)$. Bei beliebigem ν und $0 \leqq \alpha < 1$ gilt dann

$$|\{x\varepsilon_a\} - \alpha| < \varepsilon_a < \varepsilon$$

für mindestens ein ganzes x mit $\nu \leqq x \leqq \nu + [\varepsilon_a^{-1}]$. Damit ist unser Satz für $k = 1$ bewiesen. Nun wenden wir uns dem Schluß von $k-1$ auf k zu.

Es seien die Zahlen $\alpha_1, \alpha_2, \ldots, \alpha_k$ gegeben. Wir wählen ein ν' mit

$$|\{\nu'^{\varkappa}\omega\} - \alpha_\varkappa| < \frac{\varepsilon}{3} \qquad (\varkappa = 1, 2, \ldots, k). \tag{1}$$

(Dies ist nach HARDY—LITTLEWOOD [1] möglich.) Dann wählen wir weitere $\left[\frac{3}{\varepsilon} + 1\right] = N$ ganze Zahlen S_r $(r = 1, 2, \ldots, N)$ mit folgenden Eigenschaften:

$$\{S_r^k\omega\} \in J_r \qquad (r = 1, 2, \ldots, N), \tag{2}$$

wobei J_r das Intervall $\left(\frac{r-1}{N}, \frac{r}{N}\right)$ bedeutet;

$$\{S_r^{\varkappa}\omega\} < \frac{\varepsilon}{3 \cdot 3^k \nu'^{k-1}} \qquad (r = 1, 2, \ldots, N;\ \varkappa = 1, 2, \ldots, (k-1)) \tag{3}$$

((2) und (3) können, ebenfalls nach HARDY—LITTLEWOOD [1], erfüllt werden).

Nehmen wir an, unser Satz ist bis $k-1$ schon bewiesen; daraus folgt insbesondere, daß es zu einem beliebigen $\varepsilon' > 0$ ein $m' = m'(\omega, \varepsilon', k)$ gibt derart, daß bei beliebigem ν für mindestens ein ganzes n mit $\nu \leqq n \leqq \nu + m'$ die Relationen

$$\{n^{\varkappa}\omega\} < \varepsilon' \qquad (\varkappa = 1, 2, \ldots, (k-1))$$

gleichzeitig gelten. Es existiert also eine Folge ganzer Zahlen ν_ϱ $(\varrho = 1, 2, \ldots)$, für deren sämtliche Glieder die Relationen

$$\{\nu_\varrho^{\varkappa}\omega\} < \varepsilon' \qquad (\varkappa = 1, 2, \ldots, (k-1);\ \varrho - 1, 2, \ldots) \tag{4}$$

und

$$\nu_\varrho - \nu_{\varrho-1} \leqq m' \qquad (\varrho = 1, 2, \ldots) \tag{5}$$

gelten. Wir setzen

$$\varepsilon' \leqq \frac{\varepsilon}{3 \cdot 3^k \max(\nu'^{k-1}, S_1^{k-1}, \ldots, S_N^{k-1})}; \tag{6}$$

dazu gehört nach der Induktionsvoraussetzung ein m' mit (5).

Nun betrachten wir $\{\nu_\varrho^k\omega\}$ bei gegebenem ϱ. Wir wählen diejenige der Zahlen S_r, für welche J_r den Punkt $1 - \{\nu_\varrho^k\omega\}$ enthält.

Es wird nun behauptet, daß die Relationen

$$\{(\nu' + S_r + \nu_\varrho)^{\varkappa}\} = \alpha_\varkappa + \vartheta\varepsilon \qquad (\varkappa = 1, 2, \ldots, k) \tag{7}$$

mit $|\vartheta| \leqq 1$ stattfinden. (Hier und im folgenden bedeutet ϑ immer eine zwischen -1 und 1 gelegene Zahl. In verschiedenen Formeln braucht ϑ nicht dieselbe Zahl zu bedeuten.) Ist (7) bewiesen, so sind wir fertig, da dann wegen (5) und wegen der Endlichkeit der Anzahl von $\nu', S_1, \ldots, S_N$

$$m = m' + \max(S_1, S_2, \ldots, S_N)$$

gesetzt werden kann.

Der Beweis von (7) kann nun folgendermaßen geführt werden: Der Gesamtbeitrag der „gemischten“ Terme (d. h. der Terme, die keine reinen $\varkappa$-ten Potenzen sind) der Polynomentwicklung von $(\nu' + S_r + \nu_\varrho)^\varkappa$ in

$$\{(\nu' + S_r + \nu_\varrho)^\varkappa \omega\}$$

ist kleiner, als $\frac{\varepsilon}{3}$. Es ist nämlich

$$(\nu' + S_r + \nu_\varrho)^\varkappa = \sum_{\substack{0 \leqq a,\, b,\, c \leqq \varkappa \\ a+b+c=\varkappa}} \frac{\varkappa!}{a!\, b!\, c!} \nu'^a S_r^b \nu_\varrho^c;$$

für jedes „gemischte“ Term mit $c \neq 0$ gilt wegen (4) und (6)

$$\left\rbrace \frac{\varkappa!}{a!\, b!\, c!} \nu'^a S_r^b \nu_\varrho^c \omega \right\lbrace = \left\rbrace \frac{\varkappa!}{a!\, b!\, c!} \nu'^a S_r^b \{\nu_\varrho^c \omega\} \right\lbrace <$$

$$< \left\rbrace \frac{\varkappa!}{a!\, b!\, c!} \max(\nu_1'^{k-1}, S_1^{k-1}, \ldots, S_N^{k-1})\, \varepsilon' \right\lbrace \leqq \frac{\varkappa!}{3^\varkappa a!\, b!\, c!} \cdot \frac{\varepsilon}{3};$$

(man darf den Faktor $\frac{\varkappa!}{3^\varkappa a!\, b!\, c!}$ vor das Zeichen $\{\ \}$ herausheben, weil, falls $x < 1$, $u < 1$, offenbar $\{ux\} = u\{x\}$ gilt); ist $c = 0$, so muß $a \neq 0$, $b \neq 0$ sein, weil es sich sonst um kein „gemischtes“ Term handeln würde. Für diese Glieder gilt wegen (3)

$$\left\rbrace \frac{\varkappa!}{a!\, b!} \nu'^a S_r^b \omega \right\lbrace = \left\rbrace \frac{\varkappa!}{a!\, b!} \nu'^a \{S_r^b \omega\} \right\lbrace < \left\rbrace \frac{\varkappa!}{a!\, b!} \nu'^a \frac{\varepsilon}{3 \cdot 3^k \nu'^{k-1}} \right\lbrace \leqq \frac{\varkappa!}{3^\varkappa a!\, b!} \cdot \frac{\varepsilon}{3}.$$

Der Gesamtbeitrag sämtlicher „gemischter“ Terme ist also kleiner, als

$$\frac{\varepsilon}{3 \cdot 3^\varkappa} \sum_{\substack{0 \leqq a,\, b,\, c \leqq \varkappa \\ a+b+c=\varkappa}} \frac{\varkappa!}{a!\, b!\, c!} = \frac{\varepsilon}{3}.$$

Daher gilt

$$\{(\nu' + S_r + \nu_\varrho)^\varkappa \omega\} = \left\rbrace (\nu'^\varkappa + S_r^\varkappa + \nu_\varrho^\varkappa)\, \omega + \vartheta \frac{\varepsilon}{3} \right\lbrace \qquad (\varkappa = 1, 2, \ldots, k).$$

Für $\varkappa = 1, 2, \ldots, (k-1)$ gilt wegen (1), (3), (4) und (6)

$$\left\rbrace (\nu'^\varkappa + S_r^\varkappa + \nu_\varrho^\varkappa)\omega + \vartheta \frac{\varepsilon}{3} \right\lbrace = \left\rbrace \nu'^\varkappa \omega + \vartheta_1 \frac{\varepsilon}{9} + \vartheta_2 \frac{\varepsilon}{9} + \vartheta \frac{\varepsilon}{3} \right\lbrace = \alpha_\varkappa + \vartheta_3 \varepsilon$$

(hier haben $\vartheta_1, \vartheta_2, \vartheta_3$ dieselbe Bedeutung, wie ϑ); für $\varkappa = k$ erhält man wegen (1) und (2)

$$\left\rbrace (\nu'^k + S_r^k + \nu_\varrho^k)\omega + \vartheta \frac{\varepsilon}{3} \right\lbrace =$$

$$= \left\rbrace \alpha_k + \vartheta_1 \frac{\varepsilon}{3} + 1 - \nu_\varrho^k \omega + {} + \nu_\varrho^k \omega + \vartheta_2 \frac{\varepsilon}{3} + \vartheta \frac{\varepsilon}{3} \right\lbrace = \alpha_k + \vartheta_3 \varepsilon,$$

womit unser Satz bewiesen ist.

Es sei noch bemerkt, daß sich die obige Schlußweise ohne Änderung für mehrere linear unabhängige Irrationalzahlen durchführen läßt. Sind also $\omega_1, \omega_2, \ldots, \omega_l$ linear unabhängig, sind ferner

$$\begin{array}{c} \alpha_{11}, \alpha_{12}, \ldots, \alpha_{1k} \\ \alpha_{21}, \alpha_{22}, \ldots, \alpha_{2k} \\ \cdots\cdots\cdots \\ \alpha_{l1}, \alpha_{l2}, \ldots, \alpha_{lk} \end{array}$$

beliebige, zwischen 0 und 1 gelegene Zahlen und $\varepsilon > 0$, so gibt es ein nur von $\omega_1, \omega_2, \ldots, \omega_l$ und ε abhängiges m derart, daß bei beliebigem ν für mindestens ein n mit $\nu \leqq n \leqq \nu + m$ die Relationen

$$|\{n^\varkappa \omega_\lambda\} - \alpha_{\varkappa\lambda}| < \varepsilon \qquad (\varkappa = 1, 2, \ldots, k, \; \lambda = 1, 2, \ldots, l)$$

stattfinden. Hieraus folgt wieder auf triviale Weise: falls $P(x) = a_1 x + a_2 x^2 + \cdots + a_k x^k$ ein Polynom mit mindestens einem irrationalen Koeffizienten ist, so existiert ein m derart, daß bei beliebigem ν für mindestens ein n mit $\nu \leqq n \leqq \nu + m$

$$|P(n) - \alpha| < \varepsilon \qquad (0 < \alpha < 1; \; \varepsilon > 0)$$

erfüllt wird.

(Eingegangen am 6. Februar 1953.)

Literatur

[1] G. H. Hardy and E. J. Littlewood, Some problems on diophantine approximation, *Acta Math.*, 37 (1914), S. 156—239.

[2] V. Bergström, *Beiträge zur Theorie der endlichdimensionalen Moduln und der diophantischen Approximationen*. Diss. Lund, 1935.

[3] V. Bergström, Einige Bemerkungen zur Theorie der diophantischen Approximationen, *Comm. de l'Université de Lund*, 4 (1939).

ОБОСТРЕНИЕ ОДНОЙ ТЕОРЕМЫ ХАРДИ И ЛИТТЛЬВУДА

П. СЮС (Будапешт)

(Резюме)

Пусть ω—иррациональное число, k—натуральное число, $\alpha_1, \alpha_2, \ldots, \alpha_k$—числа, лежащие между 0 и 1.

Доказывается следующее обострение одной теоремы Харди и Литтльвуда: Для любого $\varepsilon > 0$ можно найти такое, зависящее лишь от ε, k и ω, натуральное число m, что при любом ν по меньшей мере для одного n удовлетворяется неравенство

$$|\{n^\varkappa \omega\} - \alpha_\varkappa| < \varepsilon \qquad (\varkappa = 1, 2, \ldots, k),$$

где

$$\{n^\varkappa \omega\} = n^\varkappa \omega - [n^\varkappa \omega] \quad \text{и} \quad \nu \leqq n \leqq \nu + m.$$

AN ALWAYS CONVERGENT ITERATION PROCESS

G. TARGONSZKY (Budapest)
(*Presented by* A. RÉNYI)

1. There are several well-known iteration methods for the approximate solution of equations with one unknown. Each of these assumes more or less stringent conditions on the function belonging to the equation. Therefore, it seems to be desirable to have a general method applicable to a possibly wide class of functions. In the present paper I intend to develop such a method working for all *continuous* functions without any further restrictions. As corollaries we shall get certain statements about the position of the zeros as well as an algorithm for solving algebraic equations.

2. Let $f(z)$ be a function continuous in the closed domain ("sector") S defined as follows:

(1) $$z \in S \quad \text{if} \quad |z| \leqq K, \quad \varphi_0 \leqq \arc z \leqq \varphi_1.$$

S may be, in extreme cases, a full circle or a single segment. We denote by

(2) $$\omega(x) = \sup_{\substack{z_1, z_2 \in S \\ |z_2 - z_1| \leqq x}} |f(z_2) - f(z_1)|$$

the modulus of continuity of $f(z)$. Of course, $\omega(x)$ is steadily increasing, and, $f(z)$ being uniformly continuous in S,

(3) $$\lim_{x \to 0} \omega(x) = 0.$$

Let $\varrho(x)$ be a continuous and strictly increasing function, defined for $x \geqq 0$, with the properties

(4) $$\varrho(0) = 0, \quad \varrho(x) \geqq \omega(x) \text{ if } x > 0, \text{ and } \lim_{x \to \infty} \varphi(x) = \infty.$$

Let further γ denote a positive number satisfying

(5) $$\gamma K \leqq 1.$$

Finally, we form the following function:

(6) $$\vartheta(z) = zF[\gamma \varrho_{-1}(|f(z)|)]$$

where $\varrho_{-1}(x)$ denotes the inverse function of $\varrho(x)$; $F(0) = 1$, $F(x)$ is steadily decreasing and $F(x) \geqq \dfrac{1}{1+x}$ for $x > 0$. Then we can state

THEOREM I. *If $z \in S$, the iteration sequence*

(7) $$z,\ \vartheta_1(z),\ \vartheta_2(z),\ \ldots,\ \vartheta_n(z), \ldots$$

defined by $\vartheta_n(z) = \vartheta[\vartheta_{n-1}(z)]$ and $\vartheta_0(z) = z$, is convergent. More precisely:

a) *If the segment between* 0 *and z (not containing* 0) *("the radius $0z$") is free from zeros of $f(z)$, then* (7) *tends to zero, its members remaining on $0z$.*

b) *if the radius $0z$ is not zero free, then the points representing the members of* (7) *remain on $0z$ and tend inwards to the next zero of $f(z)$, or, if z is itself a zero, then all members of* (7) *are equal to z.*

PROOF. It is known that if an iteration sequence $\{\varphi_n(z)\}$ is convergent with the limit ζ_0 and $\varphi(z)$ is continuous for $z = \zeta_0$, then

(8) $$\varphi(\zeta_0) = \zeta_0.$$

The whole iteration theory is based upon this simple, but fundamental fact. Now it is easy to see that

(9) $$\operatorname{arc} \vartheta_n(z) = \operatorname{arc} \vartheta(z) = \operatorname{arc} z \quad \text{for } n = 1, 2, \ldots$$

and

(10) $$0 \leqq |\vartheta_n(z)| \leqq |\vartheta_{n-1}(z)| \leqq \cdots \leqq |\vartheta(z)| \leqq |z| \quad \text{for } n = 1, 2, \ldots$$

Consequently, the points representing (7) tend inwards on the radius $0z$ or stay on their place. Clearly, (10) implies the existence of a limit ξ_0 of (7). Because of (8) we then have $\vartheta(\xi_0) = \xi_0$, and so $f(\xi_0) = 0$ provided $\xi_0 \neq 0$.

Therefore the limit of (7), if it is not equal to zero, is necessarily a zero of $f(z)$. On the other hand, if such a zero does not exist, then (7) tends to zero. Hence, in order to complete the proof of Theorem I, we have only to show that (7) passes no zeros of $f(z)$, but tends to the next one lying inwards. Let us denote this next zero by z_0. Then, according to (2) we obtain

$$|f(z)| = |f(z) - f(z_0)| \leqq \omega(|z - z_0|)$$

and because of (4)

(11) $$|f(z)| \leqq \varrho(|z - z_0|).$$

(5) and the hypothesis that $\varrho(x)$ is strictly increasing imply that here the right hand side does not become smaller, if we divide the argument of $\omega(x)$ by γK. The function $\varrho(x)$ is single-valued, monotone increasing and defined for $x \geqq 0$, therefore from (11) we may conclude

$$\varrho_{-1}(|f(z)|) \leqq \frac{|z - z_0|}{\gamma K}$$

By hypothesis we have $|z_0| \leqq K$ and so $\gamma \varrho_{-1}(|f(z)|) \leqq \left| \frac{z}{z_0} - 1 \right|$. But in case $\operatorname{arc} z = \operatorname{arc} z_0$ and $|z| \geqq |z_0|$ hold, $\frac{z}{z_0} = \left| \frac{z}{z_0} \right|$ is a positive number greater than

or equal to unity. Therefore we can write

$$\gamma\varrho_{-1}(|f(z)|) \leqq \left|\frac{z}{z_0}\right| - 1, \quad \frac{|z|}{1+\gamma\varrho_{-1}(|f(z)|)} \geqq |z_0|.$$

Finally, (6) implies

$$|z|F[\gamma\varrho_{-1}(|f(z)|)] = |\vartheta(z)| \geqq |z_0|.$$

By repeated applications we are led to the result:

(12) $$|\vartheta_n(z)| \geqq |z_0| \quad \text{for } n=1,2,\dots$$

whence we obtain, in fact, that the sequence (7) can pass no zero of $f(z)$. Consequently, (7) tends to the next one, as stated.

3. Let us now consider the case

(13) $$f(z) \in \mathrm{Lip}_c\, \alpha.$$

Then we can state

THEOREM II. *If $f(z) \in \mathrm{Lip}_c\, \alpha$, then we may choose*

(14) $$\vartheta(z) = zF\left[\gamma\left(\frac{f(z)}{c}\right)^{\frac{1}{\alpha}}\right] \quad \textit{with } 0<\gamma\leqq\frac{1}{K}.$$

PROOF. If (13) holds, then by definition

(15) $$\omega(x) \leqq cx^{\alpha}$$

and so we can choose $\varrho(x) = cx^{\alpha}$. After substituting this in (6), we obtain (14).

4. Let us investigate the case discussed by Theorem II. It may happen that after the first step $z \to \vartheta(z)$ in forming (7), we can find bettěr parameters γ, c, α for the smaller sector S_1 to which $\vartheta(z)$ belongs.

In this case it would be, of course, unnecessary to continue our sequence just in the same way as described above. Indeed, we can form a new function $\vartheta_{(1)}(z)$ with the new parameters. By continuing this process, we find the following scheme for the accelerated iteration process:

LEMMA. *Instead of forming a sequence according to* (7), *the zeros can be approximated in the same way by the sequence*

(16) $$\{z_n\} \quad \textit{with } z_{n+1} = \vartheta_{(n)}(z_n)$$

using

$$\vartheta_{(n)}(z) = zF\left[\gamma_n\left(\frac{|f(z)|}{c_n}\right)^{\frac{1}{\alpha_n}}\right].$$

Obvipusly, each member of this sequence is the first member of a sequence which would lead to the zeros, but in general not so quickly as (16). Applying our lemma to an arbitrary polynomial and choosing now $F(x) = \dfrac{1}{1+x}$, we find the following algorithm:

THEOREM III. *Given the polynomial* $P(z)=a_0+a_1z+\cdots+a_mz^m$, *the sequence* $\{z_n\}$ *defined by*

$$z_{n+1}=\frac{z_n}{1+\dfrac{|a_0+a_1z_n+a_2z_n^2+\cdots+a_mz_n^m|}{|a_1z_n|+2|a_2z_n^2|+\cdots+m|a_mz_n^m|}} \tag{17}$$

leads to a zero of $P(z)$, *or to zero, in the way stated by Theorem I.*

So if for all zeros z_i of $P(z)$ we have $|z_i|\leqq H$, we may choose $|z_0|=H$ and then (17) leads to the uttermost zero lying on $\varphi=\operatorname{arc} z_0$, if there exists one. So e. g. all real zeros and all imaginary zeros etc. may be calculated with the aid of this algorithm.

PROOF. For $|z|,|z'|\leqq|z_n|$ we have

$$\sup\frac{|f(z)-f(z')|}{|z-z'|}=c=\sup|f'(z)|\leqq|a_1|+2|a_2z_n|+\cdots+m|a_mz_n^{m-1}|.$$

Because of $\alpha=1$ we can now put (see (16))

$$\vartheta_{(n)}(z)=\frac{z}{1+\gamma\dfrac{|p(z)|}{c'}}\quad\text{with}\quad\gamma=\frac{1}{|z_n|}\quad\text{and}\quad c'\geqq c$$

and this leads to (17) by putting $c'=|a_1|+2|a_2z_n|+\ldots+m|a_mz_n^{m-1}|$.

Let us now apply Theorem III to the polynomial x^m-a. Then we have (see (17))

$$x_{n+1}=\frac{x_n}{1+\dfrac{x_n^m-a}{mx_n^m}}.$$

COROLLARY 1. If $a>0$ and $x_0\geqq\sqrt[m]{a}$, the sequence $\{x_n\}$ with

$$x_{n+1}=\frac{mx_n^{m+1}}{(m+1)x_n^m-a} \tag{18}$$

converges to $\sqrt[m]{a}$.

EXAMPLE 1. In calculating $\sqrt{2}$, by (18) we obtain $x_{n+1}=\dfrac{2x_n^3}{3x_n^2-2}$, and choosing $x_0=2$, the approximating values are $x_1=1{,}6$; $x_2=1{,}44$. The last one is exact up to the first decimal.

5. We shall now turn our attention to the question whether on a given radius $0z$ there are zeros or not. Let $f(z)$ satisfy the conditions in Theorem I, with the additional requirement

$$f(0)\neq 0. \tag{19}$$

Then we have

THEOREM IV. *The radius* $0z$ *contains no zero of* $f(z)$, *if and only if the series*

(20) $$\sum_{n=0}^{\infty} \vartheta_n(z)$$

is convergent.

PROOF. If (20) converges, then $\lim_{n\to\infty} \vartheta_n(z)=0$ and so, by Theorem I, statement b), $0z$ is zero free. Conversely, if $0z$ is zero free (i. e., $f(z)\neq 0$ on $0z$), then

$$\left|\frac{\vartheta_{n+1}(z)}{\vartheta_n(z)}\right| = F[\gamma\varrho_{-1}(|f(z)|)] \leqq \beta < 1.$$

So — according to CAUCHY's quotient test — (20) is absolutely convergent.

6. We now proceed to consider simultaneously all zeros of $f(z)$, lying on different radii. Let

(21) $$R[r,\varphi] = |\vartheta(re^{i\varphi})| = rF[\gamma\varrho_{-1}(|f(re^{i\varphi})|)].$$

Let further $r_0(\varphi)$ be a continuous and closed star curve around zero and P_1, P_2 two points on $r_0(\varphi)$. We consider the sector-like figure S_0 bounded by the arc $\widehat{P_1P_2}$ and the radii $\overline{0P_1}$ and $\overline{0P_2}$ (S_0 may be a single segment or the full figure bounded by $r_0(\varphi)$). The boundary of S_0 is supposed to belong to S_0. Let us form the following sequence of curves:

(22) $$r_0(\varphi),\ r_1(\varphi), \ldots,\ r_n(\varphi), \ldots$$

with

(23) $$r_{n+1}(\varphi) = R[r_n(\varphi), \varphi].$$

THEOREM V. *If* S_n *denotes the sector-like figure bounded by the curve* $r_n(\varphi)$ *in* (23) *and by the radii* $\overline{0P_1}, \overline{0P_2}$, *then*

(24) $$S_0 \supseteqq S_1 \supseteqq \cdots \supseteqq S_n \supseteqq \cdots$$

and all the members of this steadily decreasing sequence contain those and only those zeros of $f(z)$ *which belong to* S_0.

PROOF. By (9) and (10), $\vartheta(z)$ carries the points of the given curve $r_0(\varphi)$ into points lying on the same radius $0z$ such that the image point either coincides with the original one or is nearer to zero. Hence, this mapping acts merely on the modulus of the point, but not on its argument. The new modulus is given by

$$|\vartheta(z)| = R[r_0(\varphi), \varphi] = r_1(\varphi)$$

where $\varphi = \operatorname{arc} z$ is constant. Now, under this mapping the image points of the points of $r_0(\varphi)$ lie obviously on the curve $r_1(\varphi)$ between the radii $\overline{0P_1}$, $\overline{0P_2}$. Since $|\vartheta(z)| \leqq |z|$, we have $r_1(\varphi) \leqq r_0(\varphi)$, further $r_1(\varphi)$ is continuous

and a star curve. Hence Theorem I implies that S_1 contains precisely those zeros of $f(z)$ which are contained in S_0. The same inference shows that $S_0 \supseteq S_1 \supseteq \cdots \supseteq S_n \supseteq \cdots$ as well as that S_n possesses the properties stated by Theorem V, as we wished to prove.

Obviously, if $\overline{P_1 0 P_2}\sphericalangle$ equals zero, then Theorem V reduces to Theorem I.

An interesting consequence of Theorem V is

Corollary 2. *If the arcs of the zeros of $f(z)$ form a set of measure zero, then the area of S_n tends to zero, as n tends to infinity.*

Proof. The area of S_n is given by the formula

$$a_n = \frac{1}{2}\int_{\varphi_0}^{\varphi_1} r_n^2(\varphi)\,d\varphi. \tag{25}$$

Since $r_n(\varphi)$ tends with increasing n monotonously to 0 almost everywhere, it follows from a well-known property of the Lebesgue integral that

$$\lim_{n\to\infty}\int_{\varphi_0}^{\varphi_1} r_n^2(\varphi)\,d\varphi = 0$$

as stated.

In particular, Corollary 2 holds for all functions with a finite number of zeros within S_0, e. g. for all analytical functions. The essential content of Corollary 2 is that under the stated conditions the zeros can be included into a figure of an arbitrarily small area.

An immediate consequence of Corollary 2 is

Corollary 3. *The zeros of the polynomial*

$$P(z) = a_0 + a_1 z + a_2 z^2 + \cdots + a_m z^m$$

lie all inside the curve

$$r = \frac{k}{1+\dfrac{|a_0+a_1 k e^{i\varphi}+a_2 k^2 e^{2i\varphi}+\cdots+a_m k^m e^{mi\varphi}|}{|a_1|k+2|a_2|k^2+\cdots+m|a_m|k^m}} \tag{26}$$

with

$$k = 1+\frac{\max(|a_0|,|a_1|,\ldots,|a_{m-1}|)}{|a_m|}. \tag{27}$$

This result is an improvement of the well-known theorem according to which the zeros of $P(z)$ lie inside the circle $r=k$. Confining ourselves to real zeros, Corollary 3 means that the zeros lie in the interval

$$\left[\frac{-k}{1+\dfrac{|P(-k)|}{|a_1|k+\cdots+m|a_m|k^m}},\ \frac{k}{1+\dfrac{|P(k)|}{|a_1|k+\cdots+m|a_m|k^m}}\right].$$

Indeed, taking into account that the roots lie all inside the circle $r_0 = k$, we form $r_1(\varphi)$ and obtain (26). The truth of Corollary 3 follows then at once from Theorem V.

EXAMPLE 2. For the possible real roots of the polynomial $x^3 - x^2 - 4x + 4$ the classical bound is the interval $(-5, 5)$, while Corollary 3 gives the narrower interval $[-3{,}9;\ 4{,}2]$. (The roots are $x_1 = -2, x_2 = 1, x_3 = 2$.)

7. Throughout our discussions we have supposed that the function is defined and continuous in a sector with vertex 0; however, the hypothesis on the place of the vertex is not essential; for introducing the new function $\varphi(z) = f[z - z_c]$ we have to do with the old case. This simple observation shows that the only essential hypothesis that we require is the *continuity* of the function considered.

I am greatly indebted to A. RÉNYI for a remark in the formulation of Theorem I.

(Received 26 March 1953)

О НЕКОТОРОМ ВСЕГДА СХОДЯЩЕМСЯ ИТЕРАЦИОННОМ ПРОЦЕССЕ

Г. ТАРГОНСКИ (Будапешт)

(Резюме)

Итерационные методы приближённого решения уравнения дают последовательность значений, сходящихся к решению уравнения лишь если удовлетворяются некоторые условия. В работе даётся итерационный метод, сходящийся для всех непрерывных функций.

Если функция $f(z)$ непрерывна в круге $|z| \leq K$, то итерация функции $\vartheta(z) = zF[\gamma\varrho_{-1}(|f(z)|)]$ даёт сходящуюся для всех $|z| \leq K$ итерационную последовательность. Здесь $F(z)$ и $\varrho(x)$ надлежащим образом выбранные функции, γ — некоторой параметр. Точки, соответствующие элементам последовательности, сходятся по фиксированному радиусу к ближайшему корню, а в случае отсутствия последнего — к нулю. В случай $f(x) \in \mathrm{Lip}_c\,\alpha$ функции $F(x)$ и $\varrho(x)$ могут быть точно получены. Процесс может быть легко убыстрён.

Далее доказывается, что отсутствие корней на данном отрезке равносильно сходимости некоторого бесконечного итерационного ряда и что при помощи этого метода для любой непрерывной функции можно найти последовательность таких замкнутых непрерывных кривых, что область ограниченная каждой кривой, содержит все последующее кривые, но в то все время содержит и все корни данной функции, которые находятся внутри области, границей которой служит первая кривая.

Если множество корней есть множество меры нуль (например, в случае аналитической функции), то площадь области, ограниченной n-ой кривой стремится к нулю с возрастанием n.

Дальнейшие применения метода связаны с алгебраическими уравнениями.

ÜBER DIE ABSOLUTE KONVERGENZ VON ORTHOGONALEN POLYNOMREIHEN

Von

GÉZA FREUD (Budapest)

(*Vorgelegt von* G. ALEXITS)

Einleitung

Wir erinnern an folgenden Satz von S. BERNSTEIN [4]: Es sei $g(x)$ eine nach 2π periodische Funktion und $E_n(g)$ ihre beste Approximation in $(0, 2\pi)$ mittels trigonometrischer Polynome n-ter Ordnung im Tschebyscheffschen Sinne. Gilt nun

(1)
$$\sum_{n=1}^{\infty} \frac{E_n(g)}{\sqrt{n}} < \infty,$$

so ist die Fourier-Reihe von $g(x)$ überall absolut konvergent. Wie S. BERNSTEIN selbst bemerkt, (1) ist jedenfalls erfüllt, wenn

(1a)
$$\sum \frac{\omega\left(\frac{1}{n}, g\right)}{\sqrt{n}} < \infty$$

besteht, wobei $\omega(\delta, g)$ den Stetigkeitsmaß von $g(x)$ in $(0, 2\pi)$ bedeutet.[1]

Hieraus folgt, daß die Fourier-Reihe von $g(x)$ überall absolut konvergiert, wenn $g(x)$ einer Lipschitz-Bedingung mit einem Exponenten $\alpha > \frac{1}{2}$ genügt. In dieser Fassung wurde dieser Satz von G. ALEXITS [1], [2] auch auf eine Klasse von orthogonalen Polynomen übertragen. Es sei $\{P_n(x)\}$ die Folge der normierten orthogonalen Polynome im Intervall $(-1, +1)$ mit der nichtnegativen Gewichtsfunktion $w(x)$, ferner sei

(2)
$$f(x) \sim \sum_{\nu=0}^{\infty} c_\nu P_\nu(x)$$

die Orthogonalentwicklung einer in $(-1, +1)$ definierten L^2-integrierbaren Funktion $f(x)$. Der Satz von G. ALEXITS behauptet: ist

(3)
$$w(x) \leqq W(1-x^2)^{-\frac{1}{2}},$$

ferner $f \in \operatorname{Lip} \alpha$ mit $\alpha > \frac{1}{2}$, so gilt

(4)
$$\sum_{\nu=0}^{\infty} |c_\nu| < \infty.$$

[1] S. B. STEČKIN [9] zeigte, daß (1) und (1a) äquivalent sind.

Ist die Folge $\{P_n(x)\}$ an der Stelle x beschränkt, so wird offenbar auch die Orthogonalentwicklung (2) an derselben Stelle absolut konvergent.

Eine weitere Verallgemeinerung des Satzes von S. BERNSTEIN stammt von S. B. STEČKIN [8],]9]. Sei $\{\Phi_n\}$ ein in (a, b) definiertes, beliebiges, vollständiges Orthonormalsystem und

$$f(x) \sim \sum_{k=1}^{\infty} c_k \Phi_k(x) \tag{2a}$$

die Orthogonalentwicklung von $f \in L^2$. Bezeichnet

$$E_n^{(2)}(f, \Phi_n) = \left\{ \operatorname{Min} \int_a^b \left[f(x) - \sum_{k=1}^{n} a_k \Phi_k(x) \right]^2 \right\}^{\frac{1}{2}} = \left(\sum_{k=n+1}^{\infty} |c_k|^2 \right)^{\frac{1}{2}}, \tag{5}$$

so gilt

$$\sum_{n=1}^{\infty} |c_n| \leqq \frac{2}{\sqrt{3}} \sum_{n=1}^{\infty} \frac{1}{\sqrt{n}} E_n^{(2)}(f, \Phi). \tag{6}$$

Aus diesem Satz von S. B. STEČKIN kann — sowie aus dem erwähnten Satz von G. ALEXITS — nur dann auf die absolute Konvergenz der Orthogonalentwicklung selbst geschlossen werden, wenn die Orthogonalfunktionen gleichmäßig beschränkt sind.

In einer unlängst erschienenen Arbeit [6] habe ich gezeigt, daß in der Summierbarkeitstheorie der orthogonalen Polynomreihen die starke Forderung der gleichmäßigen Beschränktheit von $\{P_\nu(x)\}$ durch die schwächere Bedingung

$$\sum_{\nu=0}^{n} [P_\nu(x)]^2 = O(n) \tag{7}$$

ersetzt werden kann, und zwar ist (7) sicher erfüllt, wenn die Gewichtsfunktion $w(x)$ in einer Umgebung der Stelle x oberhalb einer positiven Schranke bleibt. In der vorliegenden Arbeit wollen wir zeigen, daß die Bedingung (7) — ähnlich, wie in der Summierbarkeitstheorie — auch für die Behandlung gewisser Probleme bezüglich der absoluten Konvergenz der Reihe (2) hinreicht.

Ein Satz über allgemeine Orthogonalentwicklungen

Sei $\Phi_n(x)$ ein vollständiges und normiertes System von orthogonalen Funktionen in $(-1, +1)$ bezüglich der Gewichtsfunktion $w(x) \geqq 0$, also

$$\int_a^b \Phi_m(x)\, \Phi_n(x)\, w(x)\, dx = \delta_{mn}.$$

Sei ferner (2a) die Orthogonalentwicklung einer mit der Gewichtsfunktion $w(x)$ L^2-integrierbaren Funktion $f(x)$ und

$$E_n^{(2)}(f, w, \Phi_n) = \left\{ \operatorname{Min} \int_{-1}^{+1} \left[f(x) - \sum_{k=1}^{n} a_k \Phi_k(x) \right]^2 w(x)\, dx \right\}^{\frac{1}{2}} = \left(\sum_{k=n+1}^{\infty} |c_k|^2 \right)^{\frac{1}{2}} \tag{5a}$$

SATZ I. *Gilt*

$$\sum_{\nu=1}^{n} |\Phi_\nu(x)|^2 \leqq Kn \tag{8}$$

und

$$\sum_{n=1}^{\infty} \frac{E_n^{(2)}(f, w, \Phi_n)}{\sqrt{n}} < \infty, \tag{9}$$

so ist (2) *an der Stelle x absolut konvergent.*

BEWEIS. Infolge (5a) und (8) gilt

$$\begin{aligned}\sum_{k=2^\nu+1}^{2^{\nu+1}} |c_k \Phi_k(x)| &\leqq \left(\sum_{2^\nu+1}^{2^{\nu+1}} [\Phi_k(x)]^2\right)^{\frac{1}{2}} \left(\sum_{2^\nu+1}^{2^{\nu+1}} |c_k|^2\right)^{\frac{1}{2}} \leqq \\ &\leqq \left(\sum_{k=1}^{2^{\nu+1}} [\Phi_k(x)]^2\right)^{\frac{1}{2}} \left(\sum_{2^\nu+1}^{\infty} |c_k|^2\right)^{\frac{1}{2}} < \sqrt{2K}\, 2^{\nu/2} E_{2^\nu}^{(2)}(f, w, \Phi_n).\end{aligned} \tag{10}$$

Wegen (9) erhält man nach einem bekannten Satze von CAUCHY[2] infolge der Monotonität der Reihenglieder:

$$\sum 2^{\nu/2} E_{2^\nu}^{(2)}(f, w, \Phi_n) < \infty;$$

dies ergibt wegen (10) eben die absolute Konvergenz von (2a).

Übergang zu orthogonalen Polynomreihen

Im weiteren betrachten wir die Entwicklung (2). Wir definieren, falls $f(x)$ stetig ist, den „trigonometrischen Stetigkeitsmodul" von $f(x)$ als

$$\omega^*(\delta, f) = \operatorname*{Max}_{|\vartheta_1 - \vartheta_2| \leqq \delta} |f(\cos \vartheta_1) - f(\cos \vartheta_2)|. \tag{11}$$

SATZ II. *Sei* $f(x)$ *stetig und*

$$\sum_{n=1}^{\infty} \frac{\omega^*\left(\frac{1}{n}, f\right)}{\sqrt{n}} < \infty. \tag{12}$$

Dann ist (2) *an jeder Stelle x, wo* (7) *erfüllt ist, absolut konvergent.*[3]

BEWEIS. Nach einem bekannten Satze von D. JACKSON gibt es ein Polynom $\pi_n(x)$ höchstens n-ten Grades, für welches im ganzen Intervall $(-1, +1)$

$$|f(x) - \pi_n(x)| < c_1 \omega^*\left(\frac{1}{n}\right)$$

[2] Der Cauchysche Reihensatz lautet: Ist $a_n \geqq a_{n+1} > \ldots > 0$, so sind Σa_n und $\Sigma 2^\nu a_{2^\nu}$ gleichzeitig konvergent oder divergent.

[3] Die Beziehung (12) ist bestimmt erfüllt, wenn in ϑ gleichmäßig

$$|f[\cos(\vartheta + h)] - f(\cos \vartheta)| \leqq c_3 |h|^{1/\varkappa} (\log |h|^{-1})^{-1} \cdot (\log \log |h|^{-1})^{-1} \ldots (\log_k |h|^{-1})^{-\varkappa} \tag{12a}$$

mit $\varkappa > 1$ besteht (wo $\log_p x = \log \log_{p-1} x$ bedeutet), insbesondere wenn $g(\vartheta) = f(\cos \vartheta)$ einer Lipschitz-Bedingung mit einem Exponenten $\alpha > 1/2$ genügt..

gilt. Hieraus folgt

$$(13)\quad E_n^{(2)}(f, w, P_n) \leqq \sqrt{\int_{-1}^{+1} [f(x)-\pi_n(x)]^2 w(x)\,dx} \leqq c_1\,\omega^*\left(\frac{1}{n}\right)\sqrt{\int_{-1}^{+1} w(x)\,dx}.$$

Aus (12) und (13) ergibt sich

$$\sum_{n=1}^{\infty} \frac{E_n^{(2)}(f, w, P_n)}{\sqrt{n}} < \infty,$$

also ist (2) nach Satz I absolut konvergent.

Schränkt man die Wahl der Gewichtsfunktion $w(x)$ etwas ein, so läßt sich mehr beweisen. Dazu benötigen wir den folgenden

HILFSSATZ I. *Es sei* $f \in L^2$,

$$(14)\qquad \omega_n^{(2)*}(\delta, f) = \{\operatorname*{Max}_{|h|\leqq\delta} \int_0^{\pi} [f[\cos(\vartheta+h)]-f(\cos\vartheta)]^2\,d\vartheta\}^{1/2}$$

und

$$(15)\qquad E_n^{(2)*}(f) = \{\operatorname{Min} \int_0^{\pi} [f(\cos\vartheta) - \sum_{k=0}^{n} a_k \cos k\vartheta]^2\,d\vartheta\}^{\frac{1}{2}};$$

dann ist

$$(16)\qquad E_n^{(2)*}(f) \leqq c_2\,\omega_n^{(2)*}\left(\frac{1}{n}, f\right).$$

BEWEIS. Bezeichnet

$$(17)\qquad f(\cos\vartheta) \sim \sum_{k=0}^{\infty} a_k \cos k\vartheta$$

die Fourierreihe der geraden Funktion $f(\cos\vartheta)$, so ist

$$(18)\qquad [E_n^{(2)*}(f)]^2 = \sum_{k=n+1}^{\infty} a_k^2$$

und es gilt die folgende Identität:

$$(19)\quad \sum_{k=1}^{\infty} |a_k|^2 \left(1-\frac{\sin\frac{k}{n}}{\frac{k}{n}}\right) = \frac{n}{\pi}\int_0^{1/n} dh \int_0^{\pi} \{f[\cos(\vartheta+h/2)] - f[\cos(\vartheta-h/2)\}^2\,d\vartheta.$$

Aus dem Verlauf der Kurve $y = \sin x$ folgt, daß es eine positive Konstante c_3 gibt, für welche die Ungleichung

$$(20)\qquad 1-\frac{\sin\frac{k}{n}}{\frac{k}{n}} \geqq c_3^{-1} \qquad (k \geqq n)$$

besteht. Hieraus folgt (16) wegen (18), (19) und (14), mit $c_2 = \frac{\pi c_3}{4}$, w. z. b. w.[4]

[4] Diesen vereinfachten Beweis dieses Hilfssatzes verdanke ich einer mündlichen Mitteilung des Prof. A. RÉNYI.

SATZ III. *Unter der Voraussetzung* (3) *und*

$$\sum_{n=1}^{\infty} \frac{\omega_n^{(2)}\left(\frac{1}{n}, f\right)}{\sqrt{n}} < \infty, \tag{21}$$

läßt sich behaupten, daß die Reihe (2) *an jeder Stelle* x, *wo* (7) *erfüllt ist, absolut konvergiert.*

Insbesondere ist (21) erfüllt, wenn (12a) (s. Fußnote [3]) im quadratischen Integralmittel besteht, oder spezieller, wenn $f(\cos\vartheta)$ als Funktion von ϑ eine Bedingung $\mathrm{Lip}\,(\alpha, 2)$ mit $\alpha > \frac{1}{2}$ erfüllt.

BEWEIS. Wegen (3) ist

$$\begin{aligned} E_n^{(2)}(f, w, P_n) &\leq W \left\{ \operatorname{Min} \int_{-1}^{+1} \left[f(x) - \sum_{k=0}^{n} \beta_k x^k \right]^2 \frac{dx}{\sqrt{1-x^2}} \right\}^{\frac{1}{2}} = \\ &= W \left\{ \operatorname{Min} \int_0^{\pi} \left[f(\cos\vartheta) - \sum_{k=0}^{n} \alpha_k \cos k\vartheta \right]^2 d\vartheta \right\}^{\frac{1}{2}} = W E_n^{(2)*}(f). \end{aligned} \tag{22}$$

Aus (16), (21), (22) folgt

$$\sum \frac{E_n^{(2)}(f, w, P_n)}{\sqrt{n}} < \infty$$

und somit ist Satz III auf Satz I zurückgeführt.

Über zwei Sätze von Zygmund und Hardy—Littlewood

A. ZYGMUND [13] hat bewiesen, daß die Fourier-Reihe einer nach 2π periodischen Funktion $g(\vartheta)$ absolut konvergiert, wenn $f(x)$ von beschränkter Schwankung und $g \in \mathrm{Lip}\,\alpha$ mit einem beliebigen $\alpha > 0$ ist. G. H. HARDY und J. E. LITTLEWOOD [7] haben gezeigt, daß hier die Bedingung $g \in \mathrm{Lip}\,\alpha$ durch die schwächere $g \in \mathrm{Lip}\,(\alpha, p)$ mit $\alpha p < 1$ ersetzt werden kann. An derselben Stelle bewiesen sie ferner, daß die Fourier-Reihe von $g(\vartheta)$ auch dann absolut konvergiert, wenn die Bedingungen $g \in \mathrm{Lip}\,(\alpha, p)$ mit $\alpha p = 1$, $p < 2$ und $f \in \mathrm{Lip}\,\beta$, $\beta > 0$ erfüllt sind. M. Z. WARASZKIEWICZ [12] hat beide letzterwähnten Sätze auf eine von O. SZÁSZ [10] stammende Verallgemeinerung des Bernsteinschen Satzes zurückgeführt. Der Satz von O. SZÁSZ ist in dem erwähnten Satz von S. B. STEĆKIN enthalten. Zuerst werden wir die beiden Sätze von HARDY—LITTLEWOOD auf orthogonale Polynomenreihen übertragen.

HILFSSATZ II. *Die nach* 2π *periodische Funktion* $g(\vartheta)$ *genüge einer der folgenden Bedingungen:*

a) $g(\vartheta)$ *ist von beschränkter Schwankung und* $g \in \mathrm{Lip}\,(\alpha, p)$ *mit* $\alpha p < 1$.

b) $g \in \mathrm{Lip}\,(\alpha, p)$ *mit* $\alpha p = 1$, $p < 2$ *und* $g \in \mathrm{Lip}\,\beta$ *mit* $\beta > 0$.

Dann ist[5]

$$\omega^{(2)}\left(\frac{1}{n}, g\right) = O(n^{-1-\delta}) \quad \textit{mit} \quad \delta > 0. \tag{23}$$

Bezüglich des Beweises dieses Hilfssatzes verweisen wir auf die Arbeit von WARASZKIEWICZ [12].

SATZ IV. *Die Funktion* $f(\cos\vartheta) = g(\vartheta)$ *soll entweder die Bedingung* a), *oder die Bedingung* b) *des Hilfssatzes II befriedigen. Genügt* $w(x)$ *der Ungleichung* (3), *so ist* (2) *an jeder Stelle* x, *wo* (7) *erfüllt ist, absolut konvergent.*

Unsere Behauptung folgt unmittelbar aus (23) und Satz III wegen

$$\omega^{(2)}\left(\frac{1}{n}, g\right) = \omega^{(2)*}\left(\frac{1}{n}, f\right).$$

Betrachten wir jetzt den Satz von ZYGMUND. Ist $f(x)$ eine Funktion beschränkter Schwankung, so ist auch $g(\vartheta) = f(\cos\vartheta)$ von beschränkter Schwankung, also gilt

$$\omega^{(1)}(\delta, g) = \sup_{|h| \leqq \delta} \int_0^{2\pi} |g(\vartheta + h) - g(\vartheta)|\, d\vartheta = O(\delta), \tag{24}$$

und hieraus folgt

$$\omega^{(2)}\left(\frac{1}{n}, f\right) \leqq \sqrt{\omega^{*}\left(\frac{1}{n}, f\right)} \cdot o(n^{-\frac{1}{2}}). \tag{25}$$

Aus (24) und (25) folgt wegen Satz IV:

SATZ V. *Wir nehmen an, daß* (3) *erfüllt,* $f(x)$ *eine Funktion von beschränkter Schwankung ist und es gilt*

$$\sum_{n=1}^{\infty} \frac{1}{n} \sqrt{\omega^{*}\left(\frac{1}{n}, f\right)} < \infty. \tag{26}$$

Dann ist (2) *an jeder Stelle* x, *wo* (7) *erfüllt ist, absolut konvergent.*

Es ist bemerkenswert, daß (26) erfüllt ist, wenn $f(\cos\vartheta)$ von beschränkter Schwankung ist und in $(0, \pi)$ gleichmäßig der Dini-Lipschitzschen Bedingung

$$|f[\cos(\vartheta + h)] - f(\cos\vartheta)| < c_4 (\log 1/|h|)^{-\alpha}$$

mit einem Exponenten $\alpha > 2$ genügt.

[5] Wie üblich, bedeutet $\omega^{(2)}(\delta, g)$ das Stetigkeitsmaß von g in der Metrik von L^2:

$$\omega^{(2)}(\delta, g) = \operatorname*{Max}_{|h| < \delta} \int_0^{2\pi} |g(\vartheta + h) - g(\vartheta)|^2\, d\vartheta.$$

Über die Abschätzung von $\sum_0^n [P_k(x)]^2$

In der Arbeit [6] haben wir Folgendes bewiesen: gilt in einem (echten oder unechten) Teilintervall (α, β) von $(-1, +1)$

$$w(x) \geqq m > 0, \tag{27}$$

so ist die Abschätzung (7) in jedem inneren Teilintervall von (α, β) gleichmäßig erfüllt. Es sei nun bemerkt, daß aus der Gleichmäßigkeit der Abschätzung (7) auf einer Punktmenge x die gleichmäßige absolute Konvergenz der Reihe (2) auf derselben Punktmenge folgt, falls die Bedingungen der Sätze II, III, IV, oder V erfüllt sind. Es scheint somit wünschenswert zu sein, eine einfache hinreichende Bedingung für das gleichmäßige Erfülltsein der Abschätzung (7) im ganzen Orthogonalitätsintervall zu geben.

HILFSSATZ III. *Ist* $\mu > 0$ *und*

$$w(x) > \mu(1-x^2)^{-\frac{1}{2}} \qquad (-1 \leqq x \leqq +1), \tag{27a}$$

so ist (7) *im ganzen Orthogonalitätsintervall* $(-1, +1)$ *gleichmäßig erfüllt.*

Der Beweis gründet sich, ebenso wie der Beweis des Satzes II der Arbeit [6], auf eine Schlußweise von P. ERDÖS und P. TURÁN ([5], Lemma II, S. 524—525). Die Funktion

$$K_n(x, x) = \sum_{k=0}^{n} [P_k(x)]^2$$

stellt nämlich das Maximum von $|\pi_n(x)|^2$ dar, falls $\pi_n(x)$ alle Polynome höchstens n-ten Grades durchläuft, welche der Ungleichung

$$\int_{-1}^{+1} |\pi_n(t)|^2 w(t)\, dt \leqq 1 \tag{28}$$

genügen (G. SZEGÖ [11], S. 38). Im weiteren bezeichne $\pi_n(t)$ dasjenige der (28) genügenden Polynome, welches den maximalen Wert $|\pi_n(x)|^2 = K_n(x, x)$ tatsächlich annimmt. Dann folgt aus (28) und (27a):

$$\mu \int_{-1}^{+1} |\pi_n(t)|^2 \frac{dt}{\sqrt{1-t^2}} \leqq 1. \tag{29}$$

Beachten wir nun, daß die Folge der im Intervall $(-1, +1)$ zur Gewichtsfunktion $(1-x^2)^{-\frac{1}{2}}$ gehörenden orthogonalen und normierten Polynome eben $\left\{ \sqrt{\frac{\pi}{2}}\, T_n(x) \right\}$ ist, wo $T_n(x)$ das n-te Tschebyscheffsche Polynom bezeichnet, so folgt wegen (29) nach dem schon benützten Szegöschen Hilfssatz die Ab-

schätzung

$$(30) \qquad \mu|\pi_n(x)|^2 = \mu \sum_{k=0}^{n} [P_k(x)]^2 \leqq \frac{2}{\pi} \sum_{k=0}^{n} [T_k(x)]^2.$$

Aus (30) und $|T_k(x)| \leqq 1$ ergibt sich endlich

$$(31) \qquad \sum_{k=0}^{n} [P_k(x)]^2 \leqq \frac{2}{\pi\mu}(n+1),$$

w. z. b. w.

SATZ VI. *Ersetzt man in den Sätzen II, III, IV, V die Bedingung* (7) *durch* (27) *bzw.* (27a), *so wird die Orthogonalentwicklung* (2) *unter denselben Voraussetzungen in jedem inneren Teilintervall von* (α, β) *bzw. im ganzen Intervall* $(-1, +1)$ *gleichmäßig absolut konvergent sein.*

(Eingegangen am 2. Februar 1953.)

Literaturverzeichnis

[1] G. ALEXITS, Sur la convergence des séries de polynomes orthogonaux, *Commentarii Math. Helv.*, **16** (1943), S. 200—208.

[2] G. ALEXITS, Sur la convergence et la sommabilité presque partout des séries de polynomes orthogonaux, *Acta Sci. Math.*, **12 B** (1950), S. 223—225.

[3] Н. И. Ахиезер, Лекции по теории аппроксимации. Гостехиздат (Москва—Ленинград, 1947).

[4] S. BERNSTEIN, Sur la convergence absolue des séries trigonométriques, *Comptes Rendus Acad. Sci. Paris,* **199** (1934), S. 397—400.

[5] P. ERDŐS and P. TURÁN, On interpolation. III, *Annals of Math.*, **41** (1940), S. 510—553.

[6] G. FREUD, Über die starke $(C, 1)$-Summierbarkeit von orthogonalen Polynomreihen, *Acta Math. Acad. Sci. Hung.*, **3** (1952), S. 83—88.

[7] G. H. HARDY and J. E. LITTLEWOOD, On the absolute convergence of Fourier series, *Journal of the London Math. Soc.*, **3** (1928), S. 250—253.

[8] С. Б. Стечкин, Об абсолютной сходимости ортогональных рядов, Успехы Матем. Наук, II, **3** (19) (1947), S. 177—178.

[9] С. Б. Стечкин, Об абсолютной сходимости ортогональных рядов. I, Математический Сборник, **29** (71) (1951), S. 225—232.

[10] O. SZÁSZ, Über den Konvergenzexponenten der Fourierschen Reihen gewisser Funktionenklassen, *Sitzungsber. der math.-phys. Klasse der Bayerischen Akad. der Wiss.*, 1922, S. 135—150.

[11] G. SZEGŐ, *Orthogonal Polynomials,* Amer. Math. Soc. Coll. Publ., vol. XXIII (New-York, 1939).

[12] M. Z. WARASZKIEWICZ, Remarque sur un théorème de M. Zygmund, *Bulletin International de l'Ac. Polonaise Classe Sci. Math. et Nat.*, 1929, S. 275—279.

[13] A. ZYGMUND, Remarque sur la convergence absolue des séries de Fourier, *Proc. of the London Math. Soc.*, (1928), S. 194—196.

ОБ АБСОЛЮТНОЙ СХОДИМОСТИ РЯДОВ ПО ОРТОГОНАЛЬНЫМ МНОГОЧЛЕНАМ

Г. ФРАЙД (Будапешт)

(Резюме)

Работа обобщает теоремы Бернштейна, О. Саса, Харди—Литтльвуда и Зигмунда об абсолютной сходимости рядов Фурье на ряды по ортогональным многочленам.

Типична следующая теорема:

Пусть функция $f(x)$ непрерывна на интервале $(-1, +1)$ и пусть

(1) $$\sum_{n=1}^{\infty} \frac{\omega^*\left(\frac{1}{n}, f\right)}{\sqrt{n}} < +\infty,$$

где

(2) $$\omega^*(\delta, f) = \max_{|\vartheta_1 - \vartheta_2| \leq \delta} |f(\cos\vartheta_1) - f(\cos\vartheta_2)|.$$

Тогда разложение функции $f(x)$ в ряд Фурье по многочленам, ортогональным по неотрицательному весу $w(x)$, абсолютно сходится в каждой точке, где последовательность ортогональных многочленов $\{P_n(x)\}$ удовлетворяет условию

(3) $$\sum_{\nu=0}^{n} [P_\nu(x)]^2 = O(n).$$

Условие (3), как это показал автор в одной предыдущей работе, всегда удовлетворяется, если $\alpha < x < \beta$ и в интервале (α, β) выполняется неравенство $w(x) > m > 0$. Дополнительно доказывается, что если $w(x) > \frac{m}{\sqrt{1-x^2}}$, где $m > 0$, то условие (3) равномерно выполняется во всём интервале $(-1, +1)$.

ÜBER DIE LEBESGUESCHEN FUNKTIONEN DER LAGRANGESCHEN INTERPOLATION

Von
GÉZA FREUD (Budapest)
(*Vorgelegt von* G. ALEXITS)

Einleitung

Es sei gegeben eine Zahlenmatrix

$$
(1)\qquad
\begin{array}{l}
x_{11} \\
x_{12} < x_{22} \\
\cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\
\cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\
x_{1n} < x_{2n} < \cdots < x_{nn} \\
\cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\
\cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot
\end{array}
$$

deren Reihen als Grundpunkte zur Lagrangeschen Interpolation dienen sollen. Es sei ferner $l_{kn}(x)$ die Grundfunktion, welche zum Grundpunkte x_{kn} der n-ten Lagrangeschen Interpolation gehört.

Nach einem bekannten Satze von E. HELLY [10] und H. HAHN [9] sind die Konvergenzeigenschaften der Interpolationsfolge

$$(2)\qquad L_n(f;x) = \sum_{k=1}^{n} f(x_{kn})\, l_{kn}(x)$$

durch die Lebesgueschen Funktionen

$$(3)\qquad \Lambda_n(x) = \sum_{k=1}^{n} |l_{kn}(x)|$$

bestimmt. Nach einem bekannten Satze (S. FABER [5], S. BERNSTEIN [3], L. FEJÉR [6]) kann man bei jeder Wahl der Grundpunktmatrix (1) eine Zahlenfolge $\xi_n \in (a, b)$ finden, so, daß

$$(4)\qquad \Lambda_n(\xi_n) > C_1 \log n$$

gilt, wo C_1 (sowie im weiteren $C_2, C_3, \ldots$) von n und x unabhängige positive Zahlen bedeuten. S. BERNSTEIN [3] zeigte auch, daß die Abschätzung (4) nicht verschärft werden kann. Wählen wir nämlich als n-te Reihe der Matrix (1) die Wurzeln des Tschebyscheffschen Polynoms $T_n(x)$, dann besteht

$$(5)\qquad \Lambda_n(x) = O(\log n)$$

gleichmäßig im Interpolationsintervall $(-1, +1)$. Später hat G. SZEGŐ gezeigt [13], daß die Abschätzung (5) in jedem inneren Teilintervall von $(-1, +1)$ auch dann gleichmäßig besteht, wenn man als Grundpunkte der Interpolation nicht die Nullstellen der Tschebyscheffschen Polynome, sondern die Nullstellen der Jacobischen Polynome $P_n^{(\alpha,\beta)}(x)$ mit festen $\alpha, \beta > -1$ wählt.

J. SHOHAT [12], ferner G. GRÜNWALD und P. TURÁN [8] haben unter allgemeineren Voraussetzungen schwächere Abschätzungen gefunden. Es sei $\{P_n(x)\}$ die Folge der normierten Orthogonalpolynome, welche im Orthogonalitätsintervall (a, b) durch eine positive Gewichtsfunktion bestimmt werden. Die Interpolationsmatrix (1) sei nun aus den Wurzeln von $P_n(x)$ gebildet. Die Resultate von SHOHAT bzw. GRÜNWALD—TURÁN lauten: Gilt im ganzem Intervall (a, b)

$$w(x) \geqq m > 0 \quad \text{bzw.} \quad w(x)\sqrt{1-x^2} \geqq m > 0,$$

so besteht

$$\Lambda_n(x) = O(\sqrt{n})$$

gleichmäßig in jedem inneren Teilintervall von (a, b) bzw. glechmäßig im abgeschlossenen Intervall $[a, b]$. Aus den Untersuchungen von L. FEJÉR [7] war diese schwächere Abschätzung für den Fall der Jacobischen Polynome schon vor der Szegőschen Arbeit bekannt.

Man ist geneigt zu erwarten, daß die von SZEGŐ für die Nullstellen der Jacobischen Polynome bewiesene Abschätzung (5) im wesentlichen auf der Orthogonalität dieser Polynome beruht. Doch werden in dem Beweis von G. SZEGŐ schwierige Sätze über die Asymptotik der Jacobischen Polynome und ihrer Derivierten zu Hilfe genommen. Im folgenden beweisen wir einen allgemeineren, über den Fall der Nullstellen der Jacobischen Polynome wesentlich weiter ragenden Satz, aus welchem das Szegősche Ergebnis als Spezialfall folgt.

SATZ I. *Die n-te Reihe der Matrix* (1) *bestehe aus den Nullstellen des durch die nichtnegative Gewichtsfunktion* $w(x) \in L$ *bestimmten normierten Orthogonalpolynoms* $P_n(x)$.

Gilt dann in einem Teilintervall (c, d) *von* (a, b)

$$0 < m \leqq w(x) \leqq M \tag{6}$$

und

$$|P_n(x)| \leqq K \qquad (n = 0, 1, 2, \ldots), \tag{7}$$

so besteht die Abschätzung (5) *gleichmäßig in jedem inneren Teilintervall von* (c, d).

Da im Falle der Jacobischen Polynome mit $\alpha, \beta > -1$ die Voraussetzungen von Satz I in jedem inneren Teilintervall von $(-1, +1)$ erfüllt sind, folgt in der Tat aus unserem Satze der Satz von G. SZEGŐ als Spezialfall.

Es sei bemerkt, daß ziemlich allgemeine hinreichende Bedingungen für das Bestehen der Ungleichung (7) bekannt sind (vgl. KOROUS [11] und SZEGŐ [13].)

Beweis des Satzes I

Da die n-te Reihe $x_{1n}, x_{2n}, \ldots, x_{nn}$ der Matrix (1) auch als Grundpunktfolge der Gaußschen mechanischen Quadratur vom Grade n mit der Gewichtsfunktion $w(x)$ betrachtet werden kann, gilt für ein beliebiges Polynom $\pi_{2n-1}(x)$ vom Grade $2n-1$

$$\int_a^b \pi_{2n-1}(x) w(x)\, dx = \sum_{k=1}^{n} \lambda_{kn} \pi_{2n-1}(x_{kn}), \tag{8}$$

wobei $\lambda_{1n}, \lambda_{2n}, \ldots, \lambda_{nn}$ die Cotesschen Zahlen dieser mechanischen Quadratur bedeuten. Hieraus folgt

$$\sum_{k=1}^{n} \lambda_{kn} = \int_a^b w(x)\, dx = C_2, \tag{9}$$

$$\sum_{k=1}^{n} \lambda_{kn} [P_{n-1}(x_{kn})]^2 = \int_a^b [P_{n-1}(x)]^2 w(x)\, dx = 1, \tag{10}$$

und wegen $l_{kn}(x_{in}) = \delta_{ik}$ auch

$$\int_a^b l_{kn}(x) \pi_n(x) w(x)\, dx = \lambda_{kn} \pi_n(x_{kn}), \tag{11}$$

wobei $\pi_n(x)$ ein Polynom höchstens n-ten Grades bezeichnet. Setzen wir in (11) der Reihe nach $\pi_n(x) = P_0(x), \pi_n(x) = P_1(x), \ldots, \pi_n(x) = P_{n-1}(x)$, dann erhalten wir die Koeffizienten der Orthogonalentwicklung von $l_{kn}(x)$ nach $\{P_n(x)\}$. Durch Anwendung der Formel von CHRISTOFFEL—DARBOUX ergibt sich somit[1]

$$l_{kn}(x) = \lambda_{kn} \sum_{\nu=0}^{n-1} P_\nu(x_{kn}) P_\nu(x) = \lambda_{kn} \frac{\alpha_{n-1}}{\alpha_n} \frac{P_{n-1}(x_{kn}) P_n(x)}{x - x_{kn}}. \tag{12}$$

Die Zahlen $\alpha_0, \alpha_1, \ldots, \alpha_n, \ldots$ sind hierbei der Reihe nach die Koeffizienten von x^n in $P_n(x)$; sie genügen nach einer elementaren Abschätzung (vgl. G. ALEXITS [1], [2]) der Ungleichung

$$0 < \frac{\alpha_{n-1}}{\alpha_n} \leqq \operatorname{Max}(|a|, |b|) = C_3. \tag{13}$$

Zunächst zwei Hilfssätze:

HILFSSATZ I. *Für die Grundpunkte x_{kn}, welche in ein festes inneres Teilintervall von (c, d) fallen, gilt gleichmäßig*

$$0 < \lambda_{kn} = O\left(\frac{1}{n}\right). \tag{14}$$

[1] Für den Spezialfall, in dem $\{x_{kn}\}$ die Wurzeln von $T_n(x)$ sind, stammt diese Formel von L. FEJÉR ([6], S. 442, (ε)).

Beweis bei P. ERDŐS und P. TURÁN [4], Lemma V, S. 530.

HILFSSATZ II. *Für die in einen beliebigen festen inneren Teilintervall von* (c,d) *fallenden* x_{kn} *und* $x_{k+1,n}$ *gilt gleichmäßig*

$$x_{k+1,n} - x_{kn} > \frac{C_4}{n}. \tag{15}$$

Der Beweis steht ebenfalls bei P. ERDŐS und P. TURÁN [4], Satz VIII, S. 538.

Außerdem folgt aus (12), (14)' und (7)

$$l_{kn}(x) = O(1) \tag{16}$$

gleichmäßig für die Werte x_{kn} und x, die in ein festes inneres Teilintervall von (c,d) fallen.

Nun sei x ein beliebiger Punkt des Intervalls $(c+h, d-h)$, man setze $c' = c+h/2$, $d' = d-h/2$, endlich seien x_{in} und $x_{i+1,n}$ die beiden, zur Stelle x nächstliegenden Grundpunkte.

Wir zerlegen die Summe (3) in drei Teile. Der erste Teil enthält die Glieder mit $k=i$ und $k=i+1$; der zweite jene Glieder, für welche x_{kn} in (c', d') fällt und von x_{in} und $x_{i+1,n}$ verschieden ist; der dritte Teil besteht aus allen übrigen Gliedern. In dieser Weise ergibt sich aus (12), (7) und (13):

$$\begin{aligned} \Lambda_n(x) &= \sum_{k=i}^{i+1} + \sum_{x_{kn}\in(c'd')}{}' + \sum_{x_{kn}\bar{\in}(c'd')} < \\ &< C_5 + |P_n(x)| \left\{ \frac{C_6}{n} \sum_{x_{kn}\in(c'd')}{}' \frac{1}{|x-x_{kn}|} + \frac{C_7}{h} \sum_{x_{kn}\bar{\in}(c'd')} \lambda_{kn} |P_{n-1}(x_{kn})| \right\}. \end{aligned} \tag{17}$$

Da wir aus der Summation Σ' die zu x nächstliegenden Grundpunkte ausgeschlossen haben, gilt

$$\sum_{x_{kn}\in(c'd')}{}' \frac{1}{|x-x_{kn}|} < 2\sum_{r=1}^{n} \frac{1}{C_4 r\, n} < C_8\, n \log n. \tag{18}$$

Andererseits folgt aus (9) und (10)

$$\sum_{x_{kn}\bar{\in}(c'd')} \lambda_{kn} |P_{n-1}(x_{kn})| < \sum_{k=1}^{n} \lambda_{kn} |P_{n-1}(x_{kn})| < \sqrt{\sum_{k=1}^{n} \lambda_{kn} \sum_{k=1}^{n} \lambda_{kn} [P_{n-1}(x_{kn})]^2} = C_2^{1/2}, \tag{19}$$

also besteht wegen (16), (17) und (18)

$$\Lambda(x) < C_5 + C_9 |P_n(x)| \log n, \tag{20}$$

woraus (5) folgt, w. z. b. w.

Konvergenz und Restglied der Interpolationsfolge

Es bedeute $p_{n-1}(x)$ das Polynom höchstens $n-1$-ten Grades, welches für eine gegebene Funktion $f(x)$ in (a,b) die beste Approximation im Tsche-

byscheffschen Sinne darstellt, und setzen wir

$$E_{n-1}(f) = \operatorname*{Max}_{x \in (a,\, b)} |f(x) - p_{n-1}(x)|. \tag{21}$$

Andererseits sei für die Matrix (1) die Abschätzung (5) an der Stelle x erfüllt. Dann erhalten wir, wie bekannt,

$$\begin{aligned} |L_n(f; x) - f(x)| &\leqq |L_n(f; x) - p_{n-1}(x)| + |p_{n-1}(x) - f(x)| \leqq \\ &\leqq |L_n(f - p_{n-1}; x)| + E_{n-1}(f) \leqq [\Lambda_n(x) + 1] E_{n-1}(f). \end{aligned} \tag{22}$$

SATZ II. *Die Funktion $f(x)$ genüge gleichmäßig im Intervall (c, d), wo die Bedingungen des Satzes I erfüllt sind, der Dini—Lipschitzschen Bedingung*

$$|f(x_2) - f(x_1)| = o(|\log |x_2 - x_1||^{-1}), \tag{23}$$

ferner sei $f(x)$ im ganzem Orthogonalitätsintervall (a, b) stetig.

Dann gilt

$$\lim_{n=\infty} L_n(f; x) = f(x) \tag{24}$$

gleichmäßig in jedem inneren Teilintervall von (c, d).

BEWEIS. Wir benützen eine triviale Verallgemeinerung des Satzes von D. JACKSON. Es gibt eine Polynomenfolge $\{q_n(x)\}$ mit folgenden Eigenschaften: Es gilt

$$\lim_{n=\infty} q_n(x) = f(x) \tag{25}$$

gleichmäßig in (a, b), ferner gleichmäßig in jedem inneren Teilintervall von (c, d), wo (6) und (7) erfüllt sind,

$$f(x) - q_n(x) = o\left(\frac{1}{\log n}\right). \tag{26}$$

In dieser Weise erhalten wir:

$$\begin{aligned} &|L_n(f; x) - f(x)| \leqq |L_n(f - p_{n-1}; x)| + o(1) \leqq \\ &\leqq \sum_{x_{kn} \in (c'\, d')} |l_{kn}(x)|\, |f(x_{kn}) - p_{n-1}(x_{kn})| + \sum_{x_{kn} \overline{\in} (c',\, d')} |l_{kn}(x)|\, |f(x_{kn} - p_{n-1}(x_{kn})| + o(1), \end{aligned} \tag{27}$$

wobei x ein innerer Punkt des Teilintervalls $(c+h, d-h)$ von (c, d) ist, und, wie bei Hilfssatz II, $c' = c + h/2$, $d' = d - h/2$ gesetzt sind. Infolge (19) strebt das zweite Glied in (27) gegen Null; aus (5) und (26) folgt somit (24), w. z. b. w.

Satz III. *Es sei $f(x)$ in (a, b) r-mal differenzierbar, und $f^{(r)}(x) \in \mathrm{Lip}\, \alpha$. Dann gilt*

$$\operatorname*{Max}_{c+h \leqq x \leqq d-h} |L_n(f; x) - f(x)| = O(n^{-r-\alpha} \log n) \tag{28}$$

gleichmäßig in jedem inneren Teilintervall $(c+h, d-h)$ von (c, d).

Der Beweis sei dem Leser überlassen.

(Eingegangen am 6. April 1953.)

Literaturverzeichnis

[1] G. Alexits, Sur la convergence des séries de polynomes orthogonaux, *Commentarii Math. Helvetici*, **16** (1943), S. 200—208.

[2] G. Alexits, Über den Annäherungsgrad der Orthogonalpolynomentwicklungen, *Acta Math. Acad. Sci. Hung.*, **3** (1952), S. 43—48.

[3] S. Bernstein, Quelques remarques sur l'interpolation, *Math. Annalen*, **79** (1918), S. 1—12.

[4] P. Erdős and P. Turán, On interpolation. III, *Annals of Math.*, **41** (1940), S. 410—553.

[5] G. Faber, Über die interpolatorische Darstellung stetiger Funktionen, *Jahresbericht der Deutschen Math. Vereinigung*, **23** (1914), S. 192—210.

[6] L. Fejér, Die Abschätzung eines Polynoms in einem Intervalle, wenn Schranken für seine Werte und ersten Ableitungswerte in einzelnen Punkten des Intervalles gegeben sind, und ihre Anwendung auf die Konvergenzfrage Hermitescher Interpolationsreihen, *Math. Zeitschr.*, **32** (1930), S. 426—457.

[7] L. Fejér, Lagrangesche Interpolation und die zugehörigen konjugierten Punkte, *Math. Annalen*, **106** (1932), S. 1—55.

[8] G. Grünwald und P. Turán, Über Interpolation, *Annali della Scuole Norm. Sup. di Pisa*, **7** (1938), S. 137—146.

[9] H. Hahn, Über das Interpolationsproblem, *Math. Zeitschr.*, **1** (1918), S. 115—142.

[10] E. Helly, Über lineare Funktionaloperationen, *Sitzungsber. der. Math. naturw. Klasse der Akad. in Wien*, Abt. IIa., **121** (1912), S. 265—297.

[11] J. Korous, O rozwoji funkcii jedné reálné proměnné v řadu jistých ortogonálních polinomů, *Rozpravy Ceske Akademie* (2), **48** (1938), S. 12.

[12] J. Shohat, On interpolation, *Annals of Math.*, **34** (1933), S. 130—146.

[13] G. Szegö, *Orthogonal Polynomials*, Amer. Math. Soc. Coll. Publ. vol. XXIII, (New-York, 1939).

О ФУНКЦИЯХ ЛЕБЕГА ИНТЕРПОЛЯЦИОННОГО ПРОЦЕССА ЛАГРАНЖА

Г. ФРАЙД (Будапешт)

(Резюме)

Пусть $l_{kn}(x)$ $(k=1,2,\ldots,n)$ основная интерполяционная функция Лагранжа, относящаяся к узлу x_{kn} принадлежащему системе узлов $\{x_{1n}, x_{2n}, \ldots, x_{nn}\}$. Если x_{in} $(i=1,2,\ldots,n)$—корни многочлена n-ной степени $P_n(x)$, принадлежащего системе многочленов, ортогональных по весу $w(x)\in L$, и в интервале (c, d), целиком лежащем внутри интервала ортогональности (a,b), $0<m\leq w(x)\leq M$ и там же $|P_n(x)|\leq K$ $(n=0,1,2,\ldots)$, то равномерно для всех значений x, принадлежащих какому-либо интервалу, целиком лежащему внутри (c, d), выполняется следующее равенство:

$$\sum_{k=1}^{n}|l_{kn}(x)|=O(\ln n).$$

Используя этот результат и применяя известные методы, автор получает теоремы о сходимости интерполяционного процесса Лагранжа и о порядке приближения интерполяционными многочленами.

ÜBER DIE BEZIEHUNG ZWISCHEN DER GAMMAFUNKTION UND DEN TRIGONOMETRISCHEN FUNKTIONEN

Von

MIKLÓS MIKOLÁS (Budapest)

(*Vorgelegt von* A. RÉNYI)

1. Es sei z eine komplexe Variable; wir bezeichnen, wie gewöhnlich, mit $\Gamma(z)$ die wohlbekannte Gammafunktion und mit $\Psi(z)$ ihre logarithmische Ableitung.

Seitdem EULER mittels dieser Funktion das Interpolationsproblem der Fakultäten gelöst hat,[1] ist sie nach den Forschungen hervorragender Mathematiker des 18-ten und 19-ten Jahrhunderts eine der wichtigsten Funktionen der Analysis geworden. Aus der klassischen Theorie der Gammafunktion seien die folgenden Tatsachen hervorgehoben: I) $\Gamma(z)$ ist eine meromorphe Funktion, definiert für jedes $z \neq 0, -1, -2, \ldots$ z. B. durch den Gaussschen Grenzwert

$$\Gamma(z) = \lim_{n \to \infty} \frac{n!\, n^z}{z(z+1)(z+2)\ldots(z+n)};$$

in den Punkten $z = -k$ hat sie einen Pol erster Ordnung mit dem Residuum $\frac{(-1)^k}{k!}$ $(k = 0, 1, 2, \ldots)$. — II) Es ist $\Gamma(n) = (n-1)!$ $(n = 1, 2, 3, \ldots)$; $\Gamma(z)$ genügt der Funktionalgleichung

$$\Gamma(z+1) = z\Gamma(z) \qquad (z \neq 0, -1, -2, \ldots) \tag{1}$$

und für jeden nicht-ganzzahligen Wert von z

$$\Gamma(z)\Gamma(1-z) = \frac{\pi}{\sin \pi z} \tag{2}$$

(sog. Ergänzungssatz). III) Dementsprechend hat man für $\Psi(z) = \frac{\Gamma'(z)}{\Gamma(z)}$ die Differenzengleichung

$$\Psi(z+1) - \Psi(z) = \frac{1}{z} \qquad (z \neq 0, -1, -2, \ldots); \tag{3}$$

[1] EULER [1], vgl. GODEFROY [1], S. 1—6.

aus (2) folgt

$$\Psi(z)-\Psi(1-z)=-\pi\operatorname{ctg}\pi z \quad (z\neq 0,\pm 1,\pm 2,\ldots). \tag{4}$$

IV) Die Mittag—Lefflersche Partialbruchzerlegung von $\Psi(z)$ lautet:

$$\Psi(z)=-\gamma-\frac{1}{z}+\sum_{\lambda=1}^{\infty}\left(\frac{1}{\lambda}-\frac{1}{z+\lambda}\right) \quad (z\neq 0,-1,-2,\ldots), \tag{5}$$

wo

$$\gamma=\lim_{n\to\infty}\left[\left(1+\frac{1}{2}+\cdots+\frac{1}{n}\right)-\log n\right] \tag{6}$$

die Eulersche Konstante bezeichnet; (5) setzt in Evidenz, daß $\Psi(z)$ an 0 und den negativen ganzen Zahlen einen Pol erster Ordnung mit dem Residuum —1 besitzt, sonst aber überall regulär ist.

Es sei noch die Integraldarstellung von EULER:

$$\Gamma(z)=\int_0^\infty e^{-t}\cdot t^{z-1}\,dt \qquad (\Re(z)>0)$$

und diejenige von LEGENDRE:

$$\Psi(z)+\gamma=\int_0^1\frac{1-t^{z-1}}{1-t}\,dt \qquad (\Re(z)>0)$$

erwähnt.[2]

(2) und (4) zeigt, daß die Gammafunktion mit den Kreisfunktionen in gewisser Weise verknüpft ist; man kann als weitere schöne Resultate in dieser Richtung ansehen: 1. einen Satz von GAUSS,[3] daß $\Psi(z)+\gamma$ sich für *rationale* Werte von z durch Kreisbogen und Logarithmen ausdrücken läßt; es ist nämlich für positive ganze $p<q$

$$\begin{aligned}\Psi\left(\frac{p}{q}\right)+\gamma=&-\log q-\frac{\pi}{2}\operatorname{ctg}\frac{p\pi}{q}+\\&+\frac{1}{2}\sum_{\nu=1}^{q-1}\cos\frac{2p\nu\pi}{q}\cdot\log\left(2-2\cos\frac{2\nu\pi}{q}\right);\end{aligned} \tag{7}$$

2. die berühmte Formel von KUMMER[4]

$$\begin{aligned}\log\Gamma(x)=&\left(\frac{1}{2}-x\right)(\gamma+\log 2)+(1-x)\log\pi-\frac{1}{2}\log\sin\pi x+\\&+\sum_{n=1}^{\infty}\frac{\log n}{n\pi}\sin(2n\pi x)\end{aligned} \tag{8}$$

und eine daraus fließende Reihenentwicklung von LERCH:[5]

[2] Ausführliche Literaturangaben findet man außer dem Handbuche von NIELSEN [1] auch in LÖSCH—SCHOBLIK [1].

[3] GAUSS [1]; vgl. NIELSEN [1], S. 22.

[4] KUMMER [1]; s. auch NIELSEN [1], S. 201 und NÖRLUND [1], S. 113.

[5] LERCH [1]; vgl. NIELSEN [1], S. 204.

$$\Psi(x) = -\Bigg[(\gamma + \log 2\pi) + \frac{\pi}{2}\operatorname{ctg}\pi x + \tag{9}$$
$$+ \sum_{m=1}^{\infty} \log\left(1 + \frac{1}{m}\right) \cdot \frac{\sin(2m+1)\pi x}{\sin \pi x}\Bigg],$$

welche für $0 < x < 1$ gelten.

Der Hauptzweck dieser Arbeit ist nun zu zeigen, daß *man $\Psi(z)$ für jedes nicht-ganze z mittels trigonometrischer (und rationaler) Funktionen allein in einer geschlossenen Form darstellen kann und zwar*[6]

$$\Psi(z) = -\left[\gamma + \frac{1}{2z} + \frac{\pi}{2}\operatorname{ctg}\pi z + \frac{\pi}{2}\int_0^1 \operatorname{tg}\frac{\pi t}{2}\left(\frac{\sin \pi z t}{\sin \pi z} - t\right) dt\right], \tag{10}$$

wobei man längs der reellen Achse integrieren soll.

Man wird sehen, daß dieser Satz uns gestattet, mehrere neue Formeln bzw. Behauptungen über die Eulersche Konstante γ und die Reihen $\sum_\lambda \frac{1}{(z+\lambda)^n}$ aufzustellen.

2. Es sei $z \neq 0, \pm 1, \pm 2, \ldots$; zum Beweise von (10) bemerken wir zunächst, daß der Integrand

$$U(z, t) = \operatorname{tg}\frac{\pi t}{2}\left(\frac{\sin \pi z t}{\sin \pi z} - t\right)$$

für $0 \leqq t < 1$ regulär ist. Was den Endpunkt $t = 1$ betrifft, so hat hier $U(z, t)$ einen endlichen Grenzwert, nämlich

$$\lim_{t \to 1} U(z, t) = \lim_{t \to 0} \operatorname{ctg}\frac{\pi t}{2}[\cos \pi z t - \operatorname{ctg}\pi z \cdot \sin \pi z t - (1 - t)] =$$
$$= \frac{2}{\pi}(1 - \pi z \operatorname{ctg}\pi z).$$

Somit ist die Existenz des Integrals $\int_0^1 U(z, t)\, dt$ (im eigentlichen Cauchyschen Sinne) gesichert; dies formt man jetzt um, indem man — dem Wesen nach durch Teilintegration — die Gleichheit

$$\frac{\pi}{2}\int_0^1 \operatorname{tg}\frac{\pi t}{2}\left(\frac{\sin \pi z t}{\sin \pi z} - t\right) dt = \frac{\pi z}{\sin \pi z}\int_0^1 \cos \pi z t \cdot \log\left(2\cos\frac{\pi t}{2}\right) dt \tag{11}$$

[6] Diese Formel ist also — im Gegensatze zu fast allen Integraldarstellungen in der Theorie der Gammafunktion — in der ganzen z-Ebene gültig und das rechts auftretende Integral ist *kein uneigentliches.* Ist $0 < z < \frac{1}{2}$, so hat jedes Glied in der Klammer (und auch der Integrand des letzten Gliedes) positives Vorzeichen.

verifiziert. Dazu werde mit $0<\xi<1$ die Differenz

$$\int_0^\xi \operatorname{tg}\frac{\pi t}{2}\left(\frac{\sin \pi z t}{\sin \pi z}-t\right)dt-\frac{2}{\pi}\int_0^\xi \log\left(2\cos\frac{\pi t}{2}\right)\left(\frac{\pi z\cos \pi z t}{\sin \pi z}-1\right)dt=$$

$$(12)\qquad =\int_0^\xi \frac{d}{dt}\left[-\frac{2}{\pi}\log\left(2\cos\frac{\pi t}{2}\right)\cdot\left(\frac{\sin \pi z t}{\sin \pi z}-t\right)\right]dt=$$

$$=-\frac{2}{\pi}\log\left(2\cos\frac{\pi\xi}{2}\right)\left(\frac{\sin \pi z\xi}{\sin \pi\xi}-\xi\right)$$

betrachtet; da der Grenzwert

$$\lim_{\xi\to 1-0}\log\left(2\cos\frac{\pi\xi}{2}\right)\left(\frac{\sin \pi z\xi}{\sin \pi z}-\xi\right)=$$

$$=-\frac{1}{2}\lim_{\xi\to 1-0}\left[\frac{\sin(\pi z\xi)-\xi\sin \pi z}{\cos\frac{\pi\xi}{2}\sin \pi z}\cdot\frac{\log\dfrac{1}{2\cos\frac{\pi\xi}{2}}}{\dfrac{1}{2\cos\frac{\pi\xi}{2}}}\right]=0$$

ausfällt, zeigt (12), daß

$$(13)\qquad \int_0^1 \log\left(2\cos\frac{\pi t}{2}\right)\left(\frac{\pi z\cos \pi z t}{\sin \pi z}-1\right)dt=$$

$$=\lim_{\xi\to 1-0}\int_0^\xi \log\left(2\cos\frac{\pi t}{2}\right)\left(\frac{\pi z\cos \pi z t}{\sin \pi z}-1\right)dt$$

vorhanden und gleich $\frac{\pi}{2}\int_0^1 U(z,t)\,dt$ ist. Beachtet man noch die von der Reihenentwicklung

$$(14)\qquad \log(2\sin \pi u)=-\sum_{\lambda=1}^{\infty}\frac{\cos 2\lambda\pi u}{\lambda}\qquad (0<u<1)$$

sofort ablesbaren, wohlbekannten Relationen:

$$(15)\qquad \int_0^1 \log\left(2\cos\frac{\pi t}{2}\right)dt=2\int_0^{\frac{1}{2}}\log(2\sin \pi u)\,du=0,$$

so kommt man in der Tat zu (11).

Um das uneigentliche Integral rechts in (11) auszuwerten, benützen wir nun eine interessante Folgerung des Parsevalschen Theorems für trigonometrische Reihen, nämlich die Formel

$$(16)\qquad \int_0^{2\pi} f(x)\log\left(2\sin\frac{x}{2}\right)dx=-\pi\sum_{\lambda=1}^{\infty}\frac{a_\lambda}{\lambda},$$

wo $f(x)$ eine beliebige, nach RIEMANN quadratisch integrierbare Funktion und a_λ den zu $\cos\lambda x$ gehörigen Koeffizienten in ihrer Fourierreihe bedeutet ($\lambda = 1, 2, \ldots$).[7] Daraus folgt durch die Substitution $x = \pi(1-t)$: es gilt für jede in $\langle -1, 1\rangle$ quadratisch integrierbare und *gerade* Funktion $\varphi(t)$ die Entwicklung

$$(17)\qquad \int_0^1 \varphi(t)\log\left(2\cos\frac{\pi t}{2}\right)dt = \sum_{\lambda=1}^{\infty}\frac{(-1)^{\lambda-1}}{\lambda}\int_0^1 \varphi(t)\cos\lambda\pi t\,dt;$$

wendet man dies auf den Real- und Imaginärteil von $\cos\pi z t$ an, so entsteht

$$(18)\qquad \int_0^1 \cos\pi z t\cdot\log\left(2\cos\frac{\pi t}{2}\right)dt = \sum_{\lambda=1}^{\infty}\frac{(-1)^{\lambda-1}}{\lambda}\int_0^1 \cos\pi z t\cdot\cos\lambda\pi t\,dt,$$

d. h., unter Beachtung von (5),

$$\int_0^1 \cos\pi z t\cdot\log\left(2\cos\frac{\pi t}{2}\right)dt = \frac{1}{2}\sum_{\lambda=1}^{\infty}\frac{(-1)^{\lambda-1}}{\lambda}\int_0^1 [\cos\pi t(z+\lambda) +$$

$$(19)\qquad +\cos\pi t(z-\lambda)]\,dt = \frac{1}{2\pi}\sum_{\lambda=1}^{\infty}\frac{(-1)^{\lambda-1}}{\lambda}\left[\frac{\sin\pi(z+\lambda)}{z+\lambda}+\frac{\sin\pi(z-\lambda)}{z-\lambda}\right] =$$

$$= -\frac{\sin\pi z}{2\pi z}\sum_{\lambda=1}^{\infty}\left[\left(\frac{1}{\lambda}-\frac{1}{z+\lambda}\right)+\left(\frac{1}{\lambda}+\frac{1}{z-\lambda}\right)\right] =$$

$$= -\frac{\sin\pi z}{2\pi z}\,[2\gamma+\Psi(z)+\Psi(-z)].$$

(11) und (19) haben

$$(20)\qquad \frac{1}{2}[\Psi(z)+\Psi(-z)] = -\gamma-\frac{\pi}{2}\int_0^1 \operatorname{tg}\frac{\pi t}{2}\left(\frac{\sin\pi z t}{\sin\pi z}-t\right)dt$$

zur Folge.

Andererseits gelangt man durch (3) zu

$$\Psi(1-z) = \Psi(-z)-\frac{1}{z},$$

so daß (4) in der Form:

$$(21)\qquad \frac{1}{2}[\Psi(z)-\Psi(-z)] = -\frac{1}{2z}-\frac{\pi}{2}\operatorname{ctg}\pi z$$

geschrieben werden kann.

Aus (20) und (21) ergibt sich aber nach Addition unmittelbar (10), w. z. b. w.

[7] Vgl. z. B.: ROGOSINSKI [1], S. 51.

3. Gehen wir nun zu einigen *Anwendungen* der soeben bewiesenen Formel über!

Es soll $U(z,t)$ (der Integrand in unserer Formel (10)) für ein beliebiges festes $0 \leqq t \leqq 1$ als Funktion von z allein betrachtet werden; es sei ferner $U(z,1) = \frac{2}{\pi}(1-\pi z \operatorname{ctg} \pi z)$. Man erkennt dann ohne weiteres, daß $U(z,t)$ sich in jedem Bereiche $\mathfrak{B}$, welcher keinen der Punkte $z=0, \pm 1, \pm 2, \ldots$ enthält, analytisch verhält. Gleichfalls ist offenbar, daß $U(z,t)$ auch als eine Funktion von zwei Variablen für alle Wertenpaare (z,t) von $\mathfrak{B}$ bzw. $\langle 0, 1 \rangle$ stetig ist. Somit darf man — vermöge eines bekannten Korollars des Morera-schen Satzes[8] — in $\int_0^1 U(z,t)\,dt$ unter dem Integralzeichen nach z integrieren bzw. beliebig oft differenzieren.

Wählen wir als Integrationsweg z. B. ein rektifizierbares, ganz in der längs der negativ-reellen Achse aufgeschnittenen Ebene verlaufendes, Jordan-sches Kurvenstück von $\frac{1}{2}$ bis z, auf welchem kein ganzzahliger Punkt der reellen Achse liegt, so entspringt aus (10)

$$\int_{\frac{1}{2}}^{z} \left[\Psi(u) + \frac{\pi}{2} \operatorname{ctg} \pi u\right] du = \left(\frac{1}{2} - z\right) \cdot \gamma + \frac{1}{2}\left(\log \frac{1}{2} - \log z\right) -$$

$$- \frac{\pi}{2} \int_0^1 \operatorname{tg} \frac{\pi t}{2} \left[\int_{\frac{1}{2}}^{z} \left(\frac{\sin \pi t u}{\sin \pi u} - t\right) du\right] dt,$$

falls das Zeichen „log“ überall den Hauptwert des komplexen natürlichen Logarithmus bedeutet. Laut (2) ist $\Gamma\left(\frac{1}{2}\right) = \sqrt{\pi}$, so daß die letzte Relation sich für $0 < z < 1$ in der Form

$$\log \Gamma(z) = \left(\frac{1}{2} - z\right) \cdot \gamma + \frac{1}{2} \log \frac{\pi}{2} - \frac{1}{2} \log z - \frac{1}{2} \log \sin \pi z - \tag{22}$$

$$- \frac{\pi}{2} \int_0^1 \operatorname{tg} \frac{\pi t}{2} \left[\int_{\frac{1}{2}}^{z} \left(\frac{\sin \pi t u}{\sin \pi u} - t\right) du\right] dt$$

schreiben läßt.

Durch diese Formel kann man zu einer bemerkenswerten neuen Dar-stellung der Eulerschen Konstante gelangen; nach (22) ist nämlich

[8] S. z. B.: Osgood [1], S. 307.

$$(1-2z)\cdot\gamma = \log 2 + \log\left[\frac{z\sin\pi z}{\pi}\,\Gamma(z)^2\right] - \tag{23}$$

$$-\pi\int_0^1 \operatorname{tg}\frac{\pi t}{2}\left[\int_z^{\frac{1}{2}}\left(\frac{\sin\pi t u}{\sin\pi u}-t\right)du\right]dt;$$

es sollen hierin jetzt $0 < z < \frac{1}{2}$ und das Integral nach u längs der reellen Achse genommen werden.[9] Da die Anwendung von (1) die Relation

$$\lim_{z\to 0}\left[\frac{z\sin\pi z}{\pi}\,\Gamma(z)^2\right] = \lim_{z\to 0}\left[\frac{\sin\pi z}{\pi z}(z\Gamma(z))^2\right] = \lim_{z\to 0}\Gamma(z+1)^2 = 1$$

liefert, geht (23) beim Grenzübergange $z\to 0$ über in

$$\gamma = \log 2 - \pi\int_0^1\int_0^{\frac{1}{2}} \operatorname{tg}\frac{\pi t}{2}\left(\frac{\sin\pi t u}{\sin\pi u}-t\right)du\,dt. \tag{24}$$

Wie man daher ablesen kann, *läßt sich die Differenz zwischen* γ *und* $\log 2 = 0{,}6931\ldots$ *mittels trigonometrischer Funktionen allein geschlossen ausdrücken*, was — im Vergleich zur Erklärung (6) — durchaus nicht zu erwarten war. Übrigens erweist sich der Integrand des letzten Doppelintegrals als eine *nicht-negative* Funktion von t und u, denn $\frac{\sin(\pi u t)}{t}$ nimmt im Intervalle $0 \leqq t \leqq 1$ für irgendein festes $0 < u \leqq \frac{1}{2}$ leicht nachweisbar monoton ab, und somit bleibt $\frac{\sin\pi t u}{\sin\pi u} - t$ für $0 \leqq t < 1$, $0 < u \leqq \frac{1}{2}$ positiv. Das betreffende Integral hat also gewiß positives Vorzeichen, entsprechend der wohlbekannten Tatsache, daß $\gamma < \log 2$ (genauer: $\gamma = 0{,}5772\ldots$) ist.

4. Aus (5) folgen die ebenfalls für jedes $z \neq 0, -1, -2, \ldots$ gültigen Formeln:

$$\Psi'(z+1) = \sum_{\lambda=1}^{\infty}\frac{1}{(z+\lambda)^2}, \quad \Psi''(z+1) = -2\sum_{\lambda=1}^{\infty}\frac{1}{(z+\lambda)^3}, \ldots;$$

allgemein ist

$$\Psi^{(n)}(z+1) = (-1)^{n+1}\,n!\sum_{\lambda=1}^{\infty}\frac{1}{(z+\lambda)^{n+1}} \qquad (n = 1, 2, 3, \ldots). \tag{25}$$

Ersetzt man also in (10), laut (3), $\Psi(z)$ durch $\Psi(z+1) - \frac{1}{z}$, so findet man durch n-maliges Differenzieren und nach Vergleich mit (25) die Dar-

[9] So daß hierbei sowohl t, als u *reelle* Variablen bezeichnen.

stellung

$$(26)\qquad \sum_{\lambda=1}^{\infty}\frac{1}{(z+\lambda)^{n+1}}=\frac{(-1)^{n+1}}{n!}\left[\frac{d^n}{dz^n}\left(\frac{1}{2z}-\frac{\pi}{2}\operatorname{ctg}\pi z\right)-\right.$$

$$\left.-\frac{\pi}{2}\int_0^1 \operatorname{tg}\frac{\pi t}{2}\frac{d^n}{dz^n}\left(\frac{\sin\pi z t}{\sin\pi z}\right)dt\right]\qquad (n=1,2,3,\ldots);$$

dies gilt offenbar für alle nicht-ganzzahligen z, ja sogar „in Limes" noch für $z=0,1,2,\ldots,$ weil die linke Seite auch dann regulär ist. Somit hat man insbesondere bei $z=0$:

$$(27)\qquad \zeta(n+1)=\sum_{\lambda=1}^{\infty}\frac{1}{\lambda^{n+1}}=\frac{(-1)^{n+1}}{n!}\left[\lim_{z\to 0}\frac{d^n}{dz^n}\left(\frac{1}{2z}-\frac{\pi}{2}\operatorname{ctg}\pi z\right)-\right.$$

$$\left.-\frac{\pi}{2}\int_0^1 \operatorname{tg}\frac{\pi t}{2}\lim_{z\to 0}\frac{d^n}{dz^n}\left(\frac{\sin\pi z t}{\sin\pi z}\right)dt\right]\qquad (n=1,2,3,\ldots)$$

und es ist nicht schwer, die hierin auftretenden Grenzwerte durch Heranziehung der entsprechenden Potenzreihen direkt auszuwerten.

Bekanntlich gilt[10] nämlich für $|z|<\pi$

$$z\operatorname{ctg}z=\sum_{\nu=0}^{\infty}(-1)^{\nu}\frac{2^{2\nu}B_{2\nu}}{(2\nu)!}z^{2\nu}=1-\frac{1}{3}z^2-\frac{1}{45}z^4-\frac{2}{945}z^6-\ldots,$$

wo $B_{2\nu}$ $(\nu=0,1,2,\ldots)$ die sog. Bernoullischen Zahlen[11] bezeichnen. Daraus ergibt sich sofort für jedes $z\neq 0$, welches der Ungleichung $|z|<1$ genügt:

$$(28)\qquad \frac{1}{2z}-\frac{\pi}{2}\operatorname{ctg}\pi z=\sum_{\nu=1}^{\infty}(-1)^{\nu+1}\frac{2^{2\nu}B_{2\nu}}{2(2\nu)!}\pi^{2\nu}z^{2\nu-1}$$

Beachten wir die Bedeutung der Koeffizienten laut des Cauchy—Taylorschen Entwicklungssatzes, so können wir auf

$$(29)\qquad \frac{1}{n!}\lim_{z\to 0}\frac{d^n}{dz^n}\left(\frac{1}{2z}-\frac{\pi}{2}\operatorname{ctg}\pi z\right)=\begin{cases}(-1)^{\nu+1}\dfrac{2^{2\nu-1}B_{2\nu}}{(2\nu)!}\pi^{2\nu} & \text{falls } n=2\nu-1\\ & (\nu=1,2,3,\ldots)\\ 0, & \text{wenn } n=2\nu\end{cases}$$

schließen.

Fassen wir andererseits die Generatorfunktion der *Bernoullischen Polynome* ins Auge. Ihre Entwicklung lautet:[12]

$$(30)\qquad \frac{ze^{xz}}{e^z-1}=B_0(x)+B_1(x)z+B_2(x)z^2+\cdots\qquad (|z|<2\pi);$$

[10] S. z. B.: Knopp [1], S. 431.

[11] Es ist also $B_0=1$, $B_2=\frac{1}{6}$, $B_4=-\frac{1}{30}$, $B_6=\frac{1}{42}$ usw., ferner $B_1=-\frac{1}{2}$ und $B_3=B_5=B_7=\ldots=0$; alle $B_{2\nu}$ sind rational.

[12] Vgl. z. B.: Szász [1], Bd. I, S. 697.

die Koeffizienten sind also durch

$$B_n(x) = \frac{1}{n!} \sum_{k=0}^{n} \binom{n}{k} B_k x^{n-k} \qquad (n = 0, 1, 2, \ldots) \tag{31}$$

erklärt.[13] Wir brauchen die nachstehende unmittelbare Folgerung von (30):

$$\frac{e^{z\left(x-\frac{1}{2}\right)} - e^{-z\left(x-\frac{1}{2}\right)}}{e^{\frac{z}{2}} - e^{-\frac{z}{2}}} = \frac{e^{xz}}{e^z - 1} + \frac{e^{-xz}}{e^{-z}-1} = 2[B_1(x) + B_3(x) z^2 + B_5(x) z^4 + \cdots]$$

$$(|z| < 2\pi).$$

Schreibt man da $2\pi i z$ statt z und $\frac{t+1}{2}$ statt x, so entsteht die im Einheitskreise $|z| < 1$ gültige Formel:

$$\frac{\sin \pi z t}{\sin \pi z} = 2\left[B_1\left(\frac{t+1}{2}\right) - B_3\left(\frac{t+1}{2}\right)(2\pi z)^2 + B_5\left(\frac{t+1}{2}\right)(2\pi z)^4 - + \ldots\right], \tag{32}$$

und hieraus erhält man — ebenso wie vorher — für den anderen gesuchten Grenzwert

$$\frac{1}{n!} \lim_{z \to 0} \frac{d^n}{dz^n}\left(\frac{\sin \pi z t}{\sin \pi z}\right) = \begin{cases} 0, & \text{wenn } n = 2\nu - 1, \\ (-1)^\nu 2 B_{2\nu+1}\left(\frac{t+1}{2}\right)(2\pi)^{2\nu}, & \text{falls } n = 2\nu. \end{cases} \tag{33}$$

$$(\nu = 1, 2, 3, \ldots)$$

Durch Anwendung von (29) und (33) liefert nun (27) die Formeln

$$\left.\begin{aligned} &\zeta(2\nu) = \sum_{\lambda=1}^{\infty} \frac{1}{\lambda^{2\nu}} = (-1)^{\nu-1} \frac{2^{2\nu-1} B_{2\nu}}{(2\nu)!} \pi^{2\nu} && (34) \\ &\zeta(2\nu+1) = \sum_{\lambda=1}^{\infty} \frac{1}{\lambda^{2\nu+1}} = (-1)^\nu 2^{2\nu} \pi^{2\nu+1} \int_0^1 B_{2\nu+1}\left(\frac{t+1}{2}\right) \operatorname{tg} \frac{\pi t}{2}\, dt && (35) \end{aligned}\right\} (\nu = 1, 2, 3 \ldots)$$

also *eine geschlossene Darstellung der Summen aller hyperharmonischen Reihen bei positiven ganzzahligen Exponenten* mittels der entsprechenden Potenz von π und der Bernoullischen Zahlen bzw. Polynome.

Speziell bekommt man

$$\zeta(2) = \frac{\pi^2}{6}, \quad \zeta(3) = \frac{\pi^3}{12} \int_0^1 t(1-t^2) \operatorname{tg} \frac{\pi t}{2}\, dt, \quad \zeta(4) = \frac{\pi^4}{90},$$

$$\zeta(5) = \frac{\pi^5}{720} \int_0^1 t(1-t^2)(7-3t^2) \operatorname{tg} \frac{\pi t}{2}\, dt, \quad \zeta(6) = \frac{\pi^6}{945}.$$

[13] Insbesondere ist $B_0(x) = 1$, $B_1(x) = x - \frac{1}{2}$, $B_2(x) = \frac{1}{2} x(x-1) + \frac{1}{12}$,

$$B_3(x) = \frac{1}{6} x(x-1)\left(x - \frac{1}{2}\right), \quad B_4(x) = \frac{1}{24} x^2 (x-1)^2 - \frac{1}{720},$$

$$B_5(x) = \frac{1}{120} x(x-1)\left(x - \frac{2}{1}\right)\left(x^2 - x - \frac{1}{3}\right).$$

(34) rührt, wie bekannt, von L. EULER[14] her; dagegen weiß man von $\zeta(2\nu+1)$ $(\nu=1,2,3,\ldots)$ auch heute nicht viel;[15] die letzten Ergebnisse zeigen, daß *man* (26) *als eine weitgehende Verallgemeinerung der Eulerschen Formel* (34) *ansehen mag.*

5. Mit Hilfe der Integraldarstellungen (35) wollen wir sofort eine neue Reihenrelation ableiten, welche sich auf den Zusammenhang der hyperharmonischen Reihen mit ungeraden, bzw. geraden Exponenten bezieht und so theoretisch ein gewisses Interesse hat, zugleich aber auch für numerische Zwecke brauchbar ist. Wir beweisen nämlich den Satz:

Jede Reihensumme $\zeta(2\nu+1)$ $(\nu=1,2,3,\ldots)$ *läßt sich ausschließlich mittels der unter* (34) *explizit ausgewerteten Reihensummen* $\zeta(2), \zeta(4), \zeta(6), \ldots$ *folgendermaßen darstellen:*

$$\zeta(2\nu+1)=\zeta(2\nu)\left[\frac{1}{2}A_0^{(\nu)}-\sum_{k=1}^{\infty}A_{2k}^{(\nu)}\zeta(2k)\right], \tag{36}$$

wobei

$$A_{2k}^{(\nu)}=\frac{8(2\nu)!}{B_{2\nu}}\int_0^{\frac{1}{2}}B_{2\nu+1}(x)x^{2k-1}\,dx \qquad (k=0,1,2,\ldots). \tag{37}$$

Die Koeffizienten $A_{2k}^{(\nu)}$ *besitzen die folgenden Eigenschaften:*

1. *sie sind alle positiv und rational;*
2. *es gilt für jedes* $\nu=1,2,3,\ldots$ *und* $k\geqq 1$ *die Abschätzung:*

$$A_{2k}^{(\nu)}<\frac{2}{k(2k+1)4^k}. \tag{38}$$

Der Beweis stützt sich auf die folgenden bekannten Tatsachen bezüglich der Bernoullischen Zahlen und Polynome:[16]

$$\left.\begin{aligned} &B'_{n+1}(x)=B_n(x) && (39)\\ &B_n(1-x)=(-1)^n B_n(x) && (40)\end{aligned}\right\} \qquad (n=1,2,3,\ldots)$$

$$(-1)^{\nu+1}B_{2\nu+1}(x)>0 \qquad \left(0<x<\frac{1}{2};\ \nu=0,1,2,\ldots\right) \tag{41}$$

$$B_{2\nu+1}(0)=B_{2\nu+1}\left(\frac{1}{2}\right)=B_{2\nu+1}(1)=0 \qquad (\nu=1,2,3,\ldots) \tag{42}$$

$$(-1)^{\nu+1}B_{2\nu}>0 \qquad (\nu=1,2,3,\ldots) \tag{43}$$

[14] EULER [2].

[15] Vgl. KNOPP [1], S. 246; NIELSEN [1], S. 46; NÖRLUND [1], S. 66. — NIELSEN schreibt a. a. O.: „Über die Natur der Summen $S_{2n+1}(=\zeta(2n+1))$, mit ungeradem Index, wissen wir eigentlich noch gar nichts; es ist bisher noch nicht gelungen, diese Reihen in ähnlicher Weise zu summieren, oder durch Summen derselben Gattung, aber mit niedrigerem Index, auszudrücken."

[16] Vgl. z. B.: NÖRLUND [1], Kap. 2.

(44) $$B_{2\nu}(x) = (-1)^{\nu-1} \sum_{\lambda=1}^{\infty} \frac{2\cos 2\lambda\pi x}{(2\lambda\pi)^{2\nu}}, \quad B_{2\nu+1}(x) = (-1)^{\nu+1} \sum_{\lambda=1}^{\infty} \frac{2\sin 2\lambda\pi x}{(2\lambda\pi)^{2\nu+1}}$$
$$(0 \leqq x \leqq 1;\ \nu = 1, 2, 3, \ldots).$$

Wir schicken weiter voraus, daß (28) sich unter Benutzung von (34) ersichtlich auf die einfachere Form

(45) $$\pi z \operatorname{ctg} \pi z = 1 - 2\sum_{k=1}^{\infty} \zeta(2k) z^{2k} \qquad (|z| < 1)$$

bringen läßt.

Transformieren wir nun (35) durch die Substitution $t = 1 - 2x$, so folgt auf Grund von (40):

(46) $$\zeta(2\nu+1) = (-1)^{\nu+1} (2\pi)^{2\nu+1} \int_0^{\frac{1}{2}} B_{2\nu+1}(x) \operatorname{ctg} \pi x \, dx;$$

wenn man also die Entwicklung (45) und (34) anwendet, ergibt sich

$$\zeta(2\nu+1) = (-1)^{\nu+1} 2^{2\nu+1} \pi^{2\nu} \int_0^{\frac{1}{2}} \frac{B_{2\nu+1}(x)}{x} \left[1 - 2\sum_{k=1}^{\infty} \zeta(2k) x^{2k}\right] dx =$$
$$= (-1)^{\nu+1} 2^{2\nu+1} \pi^{2\nu} \left[\int_0^{\frac{1}{2}} \frac{B_{2\nu+1}(x)}{x} \, dx - 2\sum_{k=1}^{\infty} \zeta(2k) \int_0^{\frac{1}{2}} B_{2\nu+1}(x) x^{2k-1} \, dx\right] =$$
$$= \zeta(2\nu) \left[\frac{1}{2} A_0^{(\nu)} - \sum_{k=1}^{\infty} A_{2k}^{(\nu)} \zeta(2k)\right],$$

vorausgesetzt nur, daß die ausgeführte gliedweise Integration legitim ist. Dies folgt aber unmittelbar aus den beiden Tatsachen:

1. $\langle 0, \frac{1}{2} \rangle$ ist ein Teil des Konvergenzintervalles der Potenzreihe $\sum \zeta(2k) x^{2k}$, so daß sie hierin gleichmäßig konvergiert; 2. da $B_{2\nu+1}(x)$ nach (42) bei $x = 0$ verschwindet, ist $\frac{B_{2\nu+1}(x)}{x}$ eine ganze rationale und somit in $\langle 0, \frac{1}{2} \rangle$ beschränkte Funktion.

Es bleibt noch übrig, die Behauptungen über die Koeffizienten zu verifizieren. Dazu beachte man erstens, daß $B_{2\nu+1}(x) x^{2k-1}$ sich als ein Polynom [$2(k+\nu)$-ten Grades] mit rationalen Koeffizienten erweist, und zweitens, daß wir, wegen (41) und (43), für $0 < x < \frac{1}{2}$ die Ungleichung

(47) $$\frac{B_{2\nu+1}(x)}{B_{2\nu}} > 0$$

haben; hieraus fließt zunächst die Rationalität, bzw. Positivität der Zahlenwerte $A_{2k}^{(\nu)}$ $(k=0,1,2,\ldots)$.

Um schließlich (38) zu zeigen, formen wir das Integral unter (37) durch partielle Integration um; die Benutzung von (39) und (42) ergibt:

$$\int_0^{\frac{1}{2}} B_{2\nu+1}(x)x^{2k-1}\,dx = -\frac{1}{2k}\int_0^{\frac{1}{2}} B_{2\nu}(x)x^{2k}\,dx \qquad (k=1,2,3,\ldots).$$

Nach (44) gilt aber die Abschätzung

$$|B_{2\nu}(x)| \leqq \frac{2}{(2\pi)^{2\nu}}\sum_{\lambda=1}^{\infty}\frac{1}{\lambda^{2\nu}} = \frac{|B_{2\nu}|}{(2\nu)!} \qquad (\nu=1,2,3,\ldots) \tag{48}$$

für jedes $0 \leqq x \leqq 1$; also ist

$$0 < A_{2k}^{(\nu)} \leqq \frac{8(2\nu)!}{2k}\int_0^{\frac{1}{2}}\left|\frac{B_{2\nu}(x)}{B_{2\nu}}\right| x^{2k}\,dx < \frac{8}{2k}\int_0^{\frac{1}{2}} x^{2k}\,dx = \tag{49}$$

$$= \frac{8}{2k(2k+1)2^{2k+1}} = \frac{2}{k(2k+1)4^k},$$

w. z. b. w.

Es erfordert übrigens keine Mühe, das Integral unter (37) zu berechnen und hiermit $A_{2k}^{(\nu)}$ durch die Bernoullischen Zahlen explizit auszudrücken. Schreibt man nämlich das auftretende Bernoullische Polynom in der Form (vgl. (31)):

$$B_{2\nu+1}(x) = \frac{1}{(2\nu+1)!}x^{2\nu+1} - \frac{1}{2(2\nu)!}x^{2\nu} + \frac{B_2}{2!(2\nu-1)!}x^{2\nu-1} +$$

$$+ \frac{B_4}{4!(2\nu-3)!}x^{2\nu-3} + \cdots + \frac{B_{2\nu}}{(2\nu)!\,1!}x,$$

so liefert eine gliedweise Integration:

$$A_{2k}^{(\nu)} = \frac{8(2\nu)!}{B_{2\nu}}\int_0^{\frac{1}{2}} B_{2\nu+1}(x)x^{2k-1}\,dx = \frac{1}{B_{2\nu}4^{k+\nu-1}}\left[\frac{1}{(2\nu+1)(2k+2\nu+1)} - \right. \tag{50}$$

$$\left. - \frac{1}{2(k+\nu)}\right] + \frac{1}{B_{2\nu}}\sum_{r=1}^{\nu}\binom{2\nu}{2r}\frac{B_{2r}}{(2\nu-2r+1)(2k+2\nu-2r+1)4^{k+\nu-r}}$$

$$(k=0,1,2,\ldots)$$

(38) zeigt, daß diese (nach dem Satze positiven) Zahlen bei $k\to\infty$ *schnell* gegen 0 streben, falls ν einen beliebigen fixen Wert hat; da ferner $\lim\limits_{k\to\infty}\zeta(2k)=1$ besteht, ist die Konvergenz unserer Reihenentwicklung (36) offenbar sehr gut. Dieser Umstand, nebst dem anderen, daß alle Glieder bi

auf das erste dasselbe Vorzeichen haben, macht (36) zur numerischen Berechnung von $\zeta(3), \zeta(5), \zeta(7), \ldots$ geeignet.

Es sei z. B. $\nu = 1$; dann ist nach (50)

$$A_{2k}^{(1)} = \frac{1}{B_2 4^k}\left[\frac{1}{3(2k+3)} - \frac{1}{2(k+1)}\right] + \binom{2}{2}\frac{1}{(2k+1)4^{k-1}} = \tag{51}$$
$$= \frac{1}{2^{2k-1}}\left(\frac{1}{2k+3} - \frac{3}{2k+2} + \frac{2}{2k+1}\right),$$

d. h.

$$A_0^{(1)} = \frac{5}{3}, \quad A_2^{(1)} = \frac{7}{120}, \quad A_4^{(1)} = \frac{3}{560}, \quad A_6^{(1)} = \frac{11}{16128}, \quad \ldots \tag{52}$$

und dementsprechend besteht die Entwicklung:

$$\zeta(3) = \zeta(2)\left[\frac{5}{6} - \left(\frac{7}{120}\zeta(2) + \frac{3}{560}\zeta(4) + \frac{11}{16128}\zeta(6) + \cdots\right)\right] \tag{53}$$

mit

$$\zeta(2) = \frac{\pi^2}{6} = 1{,}6449\ldots, \quad \zeta(4) = \frac{\pi^4}{90} = 1{,}0823\ldots, \quad \zeta(6) = \frac{\pi^6}{945} = 1{,}0173\ldots$$

Die ausgeschriebenen vier ersten Glieder von (52) liefern

$$\zeta(3) \approx 1{,}2022\ldots,$$

also eine Zahl, die von dem wahren Wert von $\zeta(3)\,(= 1{,}2020569\ldots)$[17] nur an der vierten Dezimalstelle um einen Fehler $< 3\cdot 10^{-4}$ abweicht.

6. Endlich sei bemerkt, daß *die Integraldarstellung* (24) *für die Eulersche Konstante eine noch einfachere Reihenentwicklung gestattet, und zwar*

$$\gamma = \log 2 - \sum_{k=1}^{\infty} \frac{1}{(2k+1)4^k}\zeta(2k+1), \tag{54}$$

mit deren Hilfe man γ bequem berechnen kann, falls $\zeta(3), \zeta(5), \zeta(7), \ldots$ schor angegeben sind.[18]

In der Tat, wenn man die Entwicklung (vgl. (32))

$$\frac{\sin \pi t u}{\sin \pi u} - t = 2\sum_{k=1}^{\infty}(-1)^k B_{2k+1}\left(\frac{t+1}{2}\right)(2\pi u)^{2k} \qquad (|u| < 1 \tag{55}$$

in (24) einsetzt, so entsteht infolge (35)

$$\log 2 - \gamma = 2\pi\int_0^1 \operatorname{tg}\frac{\pi t}{2}\int_0^{\frac{1}{2}}\sum_{k=1}^{\infty}(-1)^k B_{2k+1}\left(\frac{t+1}{2}\right)(2\pi u)^{2k}\,du\,dt =$$

[17] Vgl. Stieltjes [1].
[18] Vgl. Euler [3], S. 45.

$$=\int_0^1 (t-1)\,\mathrm{tg}\,\frac{\pi t}{2}\left[\sum_{k=1}^{\infty}(-1)^k\frac{B_{2k+1}\left(\frac{t+1}{2}\right)}{t-1}\,\frac{\pi^{2k+1}}{2k+1}\right]dt=$$

$$=\sum_{k=1}^{\infty}(-1)^k\frac{\pi^{2k+1}}{2k+1}\int_0^1 \mathrm{tg}\,\frac{\pi t}{2}\,B_{2k+1}\left(\frac{t+1}{2}\right)dt=$$

$$=\sum_{k=1}^{\infty}\frac{1}{2k+1}\,\frac{\zeta(2k+1)}{2^{2k}}.$$

Daß man beidemal gliedweise integrieren durfte, ist leicht einzusehen. Im ersten Falle handelt es sich nämlich um eine Potenzreihe, deren Konvergenzintervall die Strecke $0\leqq u\leqq\frac{1}{2}$ enthält. Was die zweite Reihe (in der Klammer) betrifft, so kommt man hierbei durch Einführung der Bezeichnung $1-t=2x$ zur Abschätzung (vgl. (40), (44))

$$\left|\frac{B_{2k+1}\left(\frac{t+1}{2}\right)}{t-1}\,\frac{\pi^{2k+1}}{2k+1}\right|=\frac{1}{2}\left|\frac{B_{2k+1}(x)}{x}\right|\frac{\pi^{2k+1}}{2k+1}= \tag{56}$$

$$=\frac{\pi}{(2k+1)2^{2k}}\left|\sum_{\lambda=1}^{\infty}\frac{\sin 2\lambda\pi x}{2\lambda\pi x}\,\frac{1}{\lambda^{2k}}\right|<\frac{\pi}{(2k+1)2^{2k}}\zeta(2k)<\frac{2\pi}{(2k+1)4^k}$$

$$(0\leqq t\leqq 1;\quad k=1,2,3,\ldots);$$

dies hat aber nach WEIERSTRASS zur Folge, daß die genannte Entwicklung, und — wegen der Beschränktheit von $(t-1)\,\mathrm{tg}\,\frac{\pi t}{2}$ in $\langle 0,1\rangle$ — auch diejenige, welche aus ihr nach Multiplikation durch $(t-1)\,\mathrm{tg}\,\frac{\pi t}{2}$ entsteht, für $0\leqq t\leqq 1$ gleichmäßig konvergieren.

(Eingegangen am 6. April 1953.)

Literatur

L. EULER [1], Brief an Goldbach von 8. I. 1730, *Corresp. Math. Phys.*, éd. P. H. Fuss 1 (1843).
[2], Institutiones calculi differentialis 2, § 122, 1755.
[3], Acta Acad. Petrop. 5, S. 45, 1781.

K. F. GAUSS [1], *Werke*, Bd. III, S. 155—156.

M. GODEFROY [1], *La fonction gamma, théorie, histoire, bibliographie* (Paris, 1901).

K. KNOPP [1], *Theorie und Anwendung der unendlichen Reihen* (Berlin—Heidelberg, 1947), IV. Auflage.

E. E. KUMMER [1], Beitrag zur Theorie der Funktion $\Gamma(x)$, *Journal für reine u. angew. Math.* 35 (1847), S. 1—4.

M. LERCH [1], Sur la différentiation des séries trigonométriques, *Comptes Rendus Acad. Sc. Paris*, 119 (1894), S. 725—728.

F. Lösch und F. Schoblik [1], *Die Fakultät (Gammafunktion) und verwandte Funktionen* (Leipzig, 1951).
N. Nielsen [1], *Handbuch der Theorie der Gammafunktion* (Leipzig, 1906).
N. E. Nörlund [1], *Differenzenrechnung* (Berlin, 1924).
W. F. Osgood [1], *Lehrbuch der Funktionentheorie* (Leipzig—Berlin, 1912).
W. Rogosinski [1], *Fouriersche Reihen*, (Berlin—Leipzig 1930), S. Göschen.
T. J. Stieltjes [1], Tables des valeurs des sommes $S_k = \sum_{n=1}^{\infty} \frac{1}{n^k}$, *Acta Math.*, **10** (1887), S. 299.
P. Szász [1], *A differenciál- és integrálszámitás elemei* (Budapest, 1951), II. Auflage.

О СВЯЗИ МЕЖДУ ГАММАФУНКЦИЕЙ И ТРИГОНОМЕТРИЧЕСКИМИ ФУНКЦИЯМИ

М. МИКОЛАШ (Будапешт)

(Резюме)

Пусть z — комплексная переменная, $\Psi(z)$ — логарифмическая производная функции $\Gamma(z)$, γ — константа Эйлера—Маскерони.

В дальнейшем прежде всего выводится на основании (5) и формулы Парсеваля новое выражение (10) для функции $\Psi(z)$, которое строится из тригонометрических, (и рациональных) функций и — в противоположность известным интегральным представлениям — справедливо для всех не целых z и не содержит несобственных интегралов.

Из многочисленных применении этого основного результата отметим следующие:

1. справедливо (22), откуда для γ получается новое выражение (24) (подинтегральная функция неотрицательна для всех рассматриваемых значений (t, u));

2. для любого фиксированного положительного n и любого не целого z справедлива формула (26), которую можно считать далекоидущим обобщением формул Эйлера (34);

3. на основании этой формулы $\zeta(3) = \sum \frac{1}{\lambda^3}$, $\zeta(5) = \sum \frac{1}{\lambda^5}$, ... могут буть представлены в замкнутом виде через соответствующую нечётную степень от π и многочлен Бернулли нечётной степени (см. (35)).

Ввиду того, что о γ и $\zeta(2\nu+1)$ $(\nu = 1, 2, \ldots)$ мы до сих пор знаем очень мало (не решён, например, вопрос о рациональности или иррациальности этих чисел), работа занимается ещё связью их между собой и проблемой выражения их через суммы $\zeta(2\nu)$ $(\nu = 1, 2, \ldots)$, явное выражение которых известно. В пункте 5 доказывается, что $\zeta(3)$, $\zeta(5)$, ... могут быть выражены через суммы гипергармонического ряда с чисто чётными показателями при рациональных коэффициентах (см. (36), (37), (38)); аналогичная связь может быть установлена между γ и $\zeta(3)$, $\zeta(5)$, ... с ещё более простыми коэффициентами (см. (54)).

ON THE FUNCTIONAL EQUATION OF DISTRIBUTIVITY

By

MIKLÓS HOSSZÚ (Miskolc)

(*Presented by* A. RÉNYI)

§ 1. Introduction

The function of two variables, $F(x, y)$, will be called *distributive* with respect to the function $G(x, y)$ if the equation

$$F[G(x, y), z] = G[F(x, z), F(y, z)] \tag{1}$$

holds. If we choose $G(x, y) = F(x, y)$, then we get the functional equation of autodistributivity which was examined by C. RYLL-NARDZEWSKI[1] in the symmetric case $F(x, y) = F(y, x)$. He has united the autodistributivity and the symmetry into the equation

$$F[x, F(y, z)] = F[F(x, y), F(z, x)] \tag{2}$$

and has proved that the most general strictly monotonic and continuous solutions of (2) are the quasiarithmetic means

$$F(x, y) = f^{-1}\left[\frac{1}{2} f(x) + \frac{1}{2} f(y)\right]$$

where $f(t)$ is an arbitrary strictly monotonic and continuous function and $f^{-1}(t)$ is its inverse function. Later B. KNASTER[2] gave an other proof by proving that all strictly monotonic and continuous functions $F(x, y)$ satisfying the functional equation (2) are

reflexive: $F(x, x) = x$;
symmetric: $F(x, y) = F(y, x)$;
bisymmetric: $F[F(x, y),\ F(u, v)] = F[F(x, u),\ F(y, v)]$

and thus, by a previous theorem of J. ACZÉL,[3] they are quasiarithmetic means.

J. ACZÉL[4] examined the functional equation of autodistributivity without supposing the symmetry of $F(x, y)$. He proved that the most general strictly

[1] C. RYLL-NARDZEWSKI, Sur les moyennes, *Studia Mathematica*, **11** (1949), pp. 31—37.

[2] B. KNASTER, Sur une équivalence pour les fonctions, *Colloquium Mathematicum*, **2** (1949), pp. 1—4.

[3] J. ACZÉL, On mean values, *Bull. Amer. Math. Soc.*, **54** (1948), pp. 392—400.

[4] J. ACZÉL, К теории средних величин (under press).

monotonic and twice differentiable solutions of the functional equation

$$F[F(x, y), z] = F[F(x, z), F(y, z)]$$

are quasilinear means

$$F(x, y) = f^{-1}[\lambda x + (1-\lambda) f(y)]$$

where $f(t)$ is an arbitrary strictly monotonic and twice differentiable function and λ is an arbitrary constant different from 1 and 0.

A. R. SCHWEITZER[5] has also treated the functional equation (1) in the special case where the functions $F(x, y)$ and $G(x, y)$ are of the form

$$f^{-1}[f(x) \pm f(y)].$$

In this paper we solve equation (1) without any additional conditions apart from strict monotony and differentiability in second order.

I am expressing my thanks to Professor J. ACZÉL for having called my attention to this problem as well as for his valuable remarks.

§ 2. The solution of the functional equation of distributivity

THEOREM. *All strictly monotonic and twice differentiable functions $F(x, y)$, $G(x, y)$ satisfying the functional equation*

$$F[G(x, y), z] = G[F(x, z), F(y, z)] \tag{1}$$

can be written in the form

$$F(x, y) = f^{-1}[f(x) g(y) + h(y)], \tag{3}$$

$$G(x, y) = f^{-1}\{f(y) + \varphi[f(x) - f(y)]\} \tag{4}$$

where the strictly monotonic and twice differentiable functions $f(t), g(t) \neq 0, h(t)$ are arbitrary and

a) *$\varphi(t)$ is an arbitrary (strictly monotonic and twice differentiable) function if $g(t) \equiv 1$;*

b) *$\varphi(-t) = -\varphi(t)$ if $g(t) \equiv -1$;*

c) *$\varphi(t) = \lambda t$ $[\lambda \neq 0, \lambda \neq 1]$ if $|g(t)| \not\equiv 1$.*

The theorem will be proved by showing that if $F(x, y)$ satisfies (1) then there exists a function $H(x, y)$ such that

$$H(x, x) = x \tag{5}$$

and

$$F[H(x, y), z] = H[F(x, z), F(y, z)] \tag{6}$$

and by reducing this equation to a functional-differential equation which has the solution (3). Finally, we get (4) as the distributive pair of $F(x, y)$.

[5] A. R. SCHWEITZER, Remarks on functional equation, *Bull. Amer. Math. Soc.*, **21** (1914), pp. 23–29.

1. The function $H(x, y)$ satisfying (5) and (6) can be constructed as follows:

(7) $$\psi(t) = G(t, t), \quad \psi[H(x, y)] = G[H(x, y), H(x, y)] = G(x, y).$$

This $H(x, y)$ is reflexive: $H(x, x) = \psi^{-1}[G(x, x)] = x$. On the other hand, if we choose in (1) $y = x = H(u, v)$ then we have

$$F\{G[H(u, v), H(u, v)], z\} = G\{F[H(u, v), z], F[H(u, v), z]\}$$

i. e. [by (7)]

$$F[G(u, v), z] = \psi\{F[H(u, v), z]\}.$$

If we compare this with

(1) $$F[G(u, v), z] = G[F(u, z), F(v, z)],$$

then we get

$$\psi\{F[H(u, v), z]\} = G[F(u, z), F(v, z)].$$

But here [cf. (7)]

$$G[F(u, z), F(v, z)] = \psi\{H[F(u, z), F(v, z)]\}$$

holds; thus we have

$$\psi\{F[H(u, v), z]\} = \psi\{H[F(u, z), F(v, z)]\}$$

and this is equivalent to (6).

2. We shall prove that if the function $F(x, y)$ satisfies the functional equation (6) with the additional condition (5), then $F(x, y)$ must be of the form (3).[6]

First we show that

(8) $$H_1(x, x)\, H_2(x, x) = a \qquad \text{(constant)}$$

where the indices $_1$ and $_2$ denote the partial differential quotient with respect to the first resp. second variable.

In order to prove (8) let us derive (6) with respect to x and y respectively:

(9) $$\begin{aligned} F_1[H(x, y), z]\, H_1(x, y) &= H_1[F(x, z), F(y, z)]\, F_1(x, z), \\ F_1[H(x, y), z]\, H_2(x, y) &= H_2[F(x, z), F(y, z)]\, F_1(y, z) \end{aligned}$$

and devide the two equations thus obtained

$$\frac{H_1(x, y)}{H_2(x, y)} = \frac{H_1[F(x, z), F(y, z)]}{H_2[F(x, z), F(y, z)]} \frac{F_1(x, z)}{F_1(y, z)}.$$

If $y = x$ then

$$\frac{H_1(x, x)}{H_2(x, x)} = \frac{H_1[F(x, z), F(x, z)]}{H_2[F(x, z), F(x, z)]} = b \qquad \text{(constant)}$$

[6] This method of proof is due to J. Aczél; see loc. cit.[4], esp. § 4.

holds. Further deriving (5) we have

$$H_1(x,x)+H_2(x,x)=1$$

and the latter equations obviously imply the validity of the equation (8).

Hereafter we derive (9) with respect to y:

$$F_{11}[H(x,y),z]\,H_1(x,y)\,H_2(x,y)+F_1[H(x,y),z]\,H_{12}(x,y)=$$
$$=H_{12}[F(x,z),F(y,z)]\,F_1(x,z)\,F_1(y,z).$$

If we put $y=x$ then taking (5) and (8) into account we have

$$F_{11}(x,z)\,a+F_1(x,z)\,H_{12}(x,x)=H_{12}[F(x,z),F(x,z)]\,F_1(x,z)^2;$$

hence we obtain

$$\frac{-1}{a}H_{12}[F(x,z),F(x,z)]\,F_1(x,z)+\frac{F_{11}(x,z)}{F_1(x,z)}=\frac{-1}{a}H_{12}(x,x).$$

Integration gives

$$-\frac{1}{a}\int_{u_0}^{F(x,z)}H_{12}(u,u)\,du+\log F_1(x,z)=-\frac{1}{a}\int_{u_0}^{x}H_{12}(u,u)\,du+\log g(z)$$

or, what is the same,

$$e^{-\frac{1}{a}\int_{u_0}^{F(x,z)}H_{12}(u,u)\,du}\,F_1(x,z)=e^{-\frac{1}{a}\int_{u_0}^{x}H_{12}(u,u)\,du}\cdot g(z).$$

Integrating again we get

$$\int_{v_0}^{F(x,z)}e^{-\frac{1}{a}\int_{u_0}^{v}H_{12}(u,u)\,du}\,dv=g(z)\int_{v_0}^{x}e^{-\frac{1}{a}\int_{u_0}^{v}H_{12}(u,u)\,du}\,dv+h(z)$$

and by denoting here

$$f(t)=\int_{v_0}^{t}e^{-\frac{1}{a}\int_{u_0}^{v}H_{12}(u,u)\,du}\,dv$$

we arrive at

$$f[F(x,z)]=g(z)f(x)+h(z)$$

where $f(t), g(t), h(t)$ are twice differentiable functions, $g(t)\neq 0$ is a consequence of the strict monotony of $F(x,y)$, and thus we have (3).

3. We shall prove that if $G(x,y)$ satisfies the functional equation (1) where $F(x,y)$ is given by (3), then $G(x,y)$ must have the form (4). To prove this we put (3) into (1):

$$f^{-1}\{f[G(x,y)]g(z)+h(z)\}=G\{f^{-1}[f(x)g(z)+h(z)],f^{-1}[f(y)g(z)+h(z)]\}.$$

By writing here the new variables x and y for $f(x)$ and $f(y)$, respectively, further, by denoting

$$\Phi(x,y)=f\{G[f^{-1}(x),f^{-1}(y)]\}, \tag{10}$$

we get

(11) $$\Phi(x, y)\, g(z)+h(z)=\Phi[x\, g(z)+h(z), y\, g(z)+h(z)].$$

Three cases are possible:

1. $g(t)\equiv 1$;
2. $g(t)\equiv -1$;
3. $|g(t)|\not\equiv 1$.

In the first case let us choose z for a given y so that $h(z)=-y$; then

(12) $$\Phi(x, y)=y+\varphi(x-y)$$

where $\varphi(t)=\Phi(t, 0)$. Clearly, this statisfies (11) with an arbitrary function $\varphi(t)$ if $g(t)\equiv 1$.

In the second case, let us choose z so that $h(z)=y$; then

$$\Phi(x, y)=y-\varphi(-x+y),$$

and putting this into (11) we see that

$$-y+\varphi(-x+y)+h(z)=-y+h(z)-\varphi(x-y)$$

which is satisfied only if $\varphi(t)$ is odd: $\varphi(-t)=-\varphi(t)$, and (12) holds again.

In the third case we prove that $\Phi(x, y)$ is reflexive:

(13) $$\Phi(t, t)=t.$$

For, if $z=z_0$ is a constant such that $|g(z_0)|\not\equiv 1$ and we choose

$$y=x=\frac{h(z_0)}{1-g(z_0)}=\frac{h}{1-g}=\gamma$$

in (11), then from the equation

$$\Phi(\gamma, \gamma)\, g+h=\Phi(\gamma, \gamma)$$

thus obtained we can express $\Phi(\gamma, \gamma)$:

$$\Phi(\gamma, \gamma)=\frac{h}{1-g}=\gamma.$$

We are returning to the equation (11) but now z is arbitrary and $y=x=\gamma$:

$$\Phi[\gamma g(z)+h(z), \gamma g(z)+h(z)]=\Phi(\gamma, \gamma)\, g(z)+h(z)=\gamma g(z)+h(z)$$

and this shows the reflexivity of $\Phi(x, y)$ for any $t(z)=\gamma g(z)+h(z)$. We remark that $t(z)\not\equiv c$ (constant), because $t(z)\equiv c$ would imply that $F(x, y)=f^{-1}[f(x)\, g(y)+h(y)]$ would be constant for $x=f^{-1}(\gamma)$, in contradiction to the strict monotony of $F(x, y)$.

If the values $t(z)$ are forming a bounded set, then using the strict monotony and continuity we can verify the reflexivity also for the values of $t_1(z)=\gamma_1 g(z)+h(z)$ where $\gamma_1=\lim\limits_{z\to\infty} t(z)=\lim\limits_{z\to\infty}[\gamma g(z)+h(z)]$ and so on until we have (13) for every t.

(13) suggests to seek for the solution of (11) in the form

(14) $$\Phi(x, y)=y+(x-y)\,\lambda(x, y).$$

As the function $\Phi(x, y)$, defined by (10), is differentiable and a fortiori continuous, therefore

$$\lambda(x, y)=\frac{\Phi(x, y)-y}{x-y}=\frac{\Phi(x, y)-\Phi(y, y)}{x-y}$$

is continuous for $x \neq y$, and for $x=y$, $\lambda(x, y)$ can be defined by

$$\lambda(y, y)=\lim_{x \to y} \lambda(x, y)=\Phi_1(y, y)$$

and hence it remains continuous here too.

Putting (14) into (11), we have

$$[y+(x-y)\lambda(x, y)]g(z)+h(z)=$$
$$=yg(z)+h(z)+[xg(z)-yg(z)]\lambda[xg(z)+h(z), yg(z)+h(z)]$$

from which with a suitable constant $z=z_0$ we get

$$\lambda(x, y)=\lambda[gx+h, gy+h], \quad |g|=|g(z_0)| \neq 1 \tag{15}$$

for all $x \neq y$, further by the continuity of $\lambda(x, y)$ also for $x=y$.

By a repeated application of (15) we arrive at

$$\lambda(x, y)=\lambda\left[g^n x+\frac{1-g^n}{1-g} h, \; g^n y+\frac{1-g^n}{1-g} h\right] \qquad (n=0, \pm 1, \pm 2, \ldots).$$

Let n tend to ∞ if $|g|<1$ resp. to $-\infty$ if $|g|>1$; then we see that

$$\lambda(x, y)=\lambda\left[\frac{h}{1-g}, \frac{h}{1-g}\right]=\lambda$$

is a constant.[7]

Taking (14) into account, we have

$$\Phi(x, y)=y+\lambda(x-y)=\lambda x+(1-\lambda) y, \tag{16}$$

and $\lambda \neq 0, \lambda \neq 1$ follow from the strict monotony.

The solutions (12) and (16) can be united into the form

$$\Phi(x, y)=y+\varphi(x-y)$$

where

a) $\varphi(t)$ is arbitrary if $g(t) \equiv 1$;

b) $\varphi(-t)=-\varphi(t)$ if $g(t) \equiv -1$;

c) $\varphi(t)=\lambda t$ $[\lambda \neq 0, \lambda \neq 1]$ if $|g(t)| \not\equiv 1$.

Finally, if we put our results in the definition (10) of $\Phi(x, y)$, then we see that $G(x, y)$ must be of the form (4).

It might be observed that we have used the continuous differentiability of $\Phi(x, y)$ only in the point $y=x=\dfrac{h(z_0)}{1-g(z_0)}$.

[7] J. Aczél has kindly called my attention to the fact that if we do not suppose the differentiability then there exist also more general solutions of (15). E. g. if $g(t) \equiv g \neq \pm 1$ is constant, then also $\lambda(x, y)=\chi[\log|x-y|]$ with an arbitrary periodic $\chi(t)=\chi[t+\log|g|]$ satisfies (15).

4. We must still verify that the functions of the forms (3), (4) with the restrictions (a), (b), (c) actually satisfy the equation (1). We put (3) and (4) into (1); then we have

$$f^{-1}(\{f(y)+\varphi[f(x)-f(y)]\}g(z)+h(z))=$$
$$=f^{-1}\{f(y)g(z)+h(z)+\varphi[f(x)g(z)-f(y)g(z)]\}.$$

If $g(z)\equiv 1$, then this equation holds for every $\varphi(t)$.

If $g(z)\equiv -1$, then the oddness (b) of $\varphi(t)$ gives

$$-\varphi[f(x)-f(y)]=\varphi[-f(x)+f(y)]$$

which secures the validity of our equation.

If $|g(z)|\not\equiv 1$, then $\varphi(t)=\lambda t$ again reduces the required equation

$$\varphi[f(x)-f(y)]g(z)=\varphi[f(x)g(z)-f(y)g(z)]$$

to an identity.

This completes the proof of our theorem.

§ 3. Remarks

1. Together with $F(x,y)$ and $G(x,y)$ also every pair of functions

$$F_*(x,y)=\alpha^{-1}\{F[\alpha(x),\beta(y)]\},$$
$$G_*(x,y)=\alpha^{-1}\{G[\alpha(x),\alpha(y)]\}$$

satisfies the equation (1). This can be verified immediately.

2. We also remark that the solution contains the pair of functions xy, $x+y$, resp xy, x^y, although xy resp. x^y is not strictly monotonic for $x=0$ or $y=0$. E. g. if

$$f(t)=h(t)=\log t,\quad g(t)\equiv 1,\quad \varphi(t)=\log(e^t+1),$$

then (3) and (4) become

$$F(x,y)=e^{\log x+\log y}=xy,$$
$$G(x,y)=e^{\log y+\log(e^{\log x-\log y}+1)}=e^{\log(x+y)}=x+y.$$

Further, with $\alpha(t)=\log t$, $\beta(t)=t$,

$$F_*(x,y)=\alpha^{-1}\{F[\alpha(x),\beta(y)]\}=e^{y\log x}=x^y,$$
$$G_*(x,y)=\alpha^{-1}\{G[\alpha(x),\alpha(y)]\}=e^{\log x+\log y}=xy.$$

3. If the function $F(x,y)$ satisfies the functional equation

$$F[G(x,y),z]=K[F(x,z),F(y,z)]$$

where the functions are strictly monotonic and twice differentiable, then $F(x,y)$ must be of the form

$$F(x,y)=k[f(x)g(y)+h(y)].$$

The proof is similar to that of (3).

The functions of this form (and only these) can be represented by nomograms with two straight scales and one curve.[8]

4. If the strictly monotonic and twice differentiable functions $F(x, y)$, $G(x, y)$ are distributive *on both sides*, that is, they satisfy the functional equation (1) and

$$F[z, G(x, y)] = G[F(z, x), F(z, y)], \tag{1'}$$

then either

$G(x, y)$ is reflexive: $G(x, x) = x$

or

$F(x, y)$ is associative: $F[F(x, y), z] = F[x, F(y, z)]$.

In fact, our theorem shows that if $g(t) \not\equiv 1$ then $\varphi(0) = 0$ and $G(x, y)$ is reflexive.

If, on the other hand, $g(t) \equiv 1$, then $F(x, y)$ has the form

$$F(x, y) = f^{-1}[f(x) + h(y)].$$

From (1') we get similarly

$$F(x, y) = f_*^{-1}[h_*(x) + f_*(y)],$$

thus

$$f^{-1}[f(x) + h(y)] = f_*^{-1}[h_*(x) + f_*(y)],$$

or, what is the same,

$$f_*[f^{-1}(x + y)] = h_*[f^{-1}(x)] + f_*[h^{-1}(y)]$$

holds if $G(x, x) \neq x$.

This can be reduced to the functional equation[9]

$$f_1(x + y) = f_2(x) + f_3(y)$$

and hence

$$h(t) = f(t) + C$$

follows easily. Therefore

$$F(x, y) = f^{-1}[f(x) + f(y) + C]$$

is in fact associative:

$$F[F(x, y), z] = F[x, F(y, z)] = f^{-1}[f(x) + f(y) + f(z) + 2C].$$

(Received 8 April 1953)

[8] The problem of characterisation of these functions by a functional equation wa[s] raised by J. Aczél in a lecture.

[9] H. W. Pexider, *Monatshefte für Math. u. Phys.*, 14 (1903), p. 293.

О ФУНКЦИОНАЛЬНОМ УРАВНЕНИИ ДИСТРИБУТИВНОСТИ

М. ГОССУ (Мишкольц)

(Резюме)

Работа содержит решение функционального уравнения

$F[G(x, y), z] = G[F(x, z), F(y, z)]$ (уравнение дистрибутивности)

при условиях строгой монотонности и двойной дифференцируемости в виде

$$F(x, y) = f^{-1}[f(x)g(y) + h(y)],$$
$$G(x, y) = f^{-1}\{f(y) + \varphi[f(x) - f(y)]\},$$

где

$f(t)$, $g(t) \not\equiv 0$, $h(t)$ любые строго монотонные и дважды дифференцируемые функции;

$\varphi(t)$ любая (строго монотонная, дважды дифференцируемая) функция, если $g(t) \equiv 1$;

$$\varphi(-t) = -\varphi(t), \quad \text{если} \quad g(t) \equiv -1;$$
$$\varphi(t) = \lambda t \ (\lambda \neq 0, \lambda \neq 1), \quad \text{если} \quad |g(t)| \not\equiv 1.$$

Проблема возникла как обобщение функционального уравнения $F[F(x, y), z] = F[F(x, z), F(y, z)]$ (уравнение автодистрибутивности), которое исследовал Я. Ацел.

ON A SPECIAL KIND OF DUALITY IN GROUP THEORY. I

By

L. FUCHS (Budapest), A. KERTÉSZ and T. SZELE (Debrecen)

(*Presented by* L. RÉDEI)

§ 1. Introduction

For a given group G we denote by $S(G)$ and $F(G)$ the manifold of all subgroups resp. the manifold of all factorgroups (or, what is the same, of all homomorphic images) of G. Both $S(G)$ and $F(G)$ are considered as systems of pairwise non-isomorphic abstract groups. If for two groups G, H the manifold $S(G)$ coincides with $F(H)$, then we say that the groups G and H are *S—F-dual*. In case $F(G)=S(H)$ the groups G and H will be called *F—S-dual*. If G and H are at the same time both S—F-dual and F—S-dual, then they are said to be *dual* groups.

An example of a pair of dual groups G and H is given by

$$G=\sum_{a} C(p^2), \quad H=C(p)+G$$

where G is a direct sum of a countable infinite number of copies of $C(p^2)$, $C(p^n)$ denoting the cyclic group of order p^n with a prime p. These groups G and H are not isomorphic. If two dual groups G and H are isomorphic or (what is essentially the same) if $G=H$, then we call the group G *selfdual*. Thus a group G is selfdual if and only if the manifold $S(G)$ coincides with $F(G)$. In this case the manifold $S(G)=F(G)$ is called the *standard manifold* of the group G.

Several problems arise in connection with this special kind of duality: Given G, whether there exists a group which is S—F-dual resp. F—S-dual to G? If so, to determine all such groups. Other problems are to determine all groups G which have a dual pair, to determine all selfdual and all pairs of dual groups.

The present paper is devoted to the discussion of these questions for *countable abelian groups.*[1] Our results are contained in Theorems 1, 2 and 3.

[1] It is easy to give an example for a selfdual non-commutative group: if p is an odd prime, then the non-commutative group of order p^3 all of whose elements are of order p is easily seen to be selfdual. (This group may be defined by the generators a, b, c connected by the defining relations

$$a^p=b^p=c^p=1, \quad a^{-1}b^{-1}ab=c, \quad ac=ca, \quad bc=cb.)$$

Let us also mention that we have observed — without having laid stress on describing

§ 2. Preliminaries

In what follows, by a group we shall always mean an additively written abelian group with more than one element. Groups will be denoted by Latin capital letters and their elements by x, a, b, c. The other small Latin letters are reserved for rational integers, in particular p for prime numbers. The subgroup generated by the elements $a, b, \dots$ of a group is denoted by $\{a, b, \dots\}$. A group every element of which is of finite order is called a *torsion group*. In the contrary case, namely if every element $\neq 0$ of a group is of infinite order, the group is said to be *torsion free*. A group which is neither a torsion group nor torsion free will be called a *mixed group*. A torsion group is the direct sum of its uniquely determined *primary components*, the latter being p-groups, i. e., groups every element of which is of p-power order. A torsion group T is said to be a *bounded group* if it has an element of maximal order; in the contrary case T is an unbounded torsion group. We denote by $A+B$ the direct sum of the groups A, B. By

$$\sum_n D \quad \text{resp.} \quad \sum_{\mathfrak{a}} D$$

we understand the direct sum of a finite number n resp. of a countable infinite number of isomorphic copies of a group D. The additive group of all rational numbers will be denoted by R, and C will denote the group R taken modulo 1, i. e., C is the group of all rotations of finite order of the circle. We denote the p-primary component of C by $C(p^\infty)$, while $C(r)$ denotes the cyclic group of order r $(1 \leq r \leq \infty)$.

By a well-known theorem (see e. g. [3])[2] every (finite or) countable abelian p-group is isomorphic to a subgroup of the group

$$\sum_{\mathfrak{a}} C(p^\infty),$$

and every (finite or) countable abelian group is isomorphic to a subgroup of the group

$$\sum_{\mathfrak{a}} (C+R).$$

Let P_p be an arbitrary p-group. Then the union of all subgroups in P_p which are direct sums of groups $C(p^\infty)$ is itself a direct sum of groups $C(p^\infty)$ and

the finite selfdual groups — that *a selfdual finite group is necessarily nilpotent*. In fact, if G is a finite selfdual group, then each Sylow-subgroup S_p of G must be a homomorphic image of G, $G/N_p \simeq S_p$ where all Sylow-groups S_q of G with $q \neq p$ are contained in N_p. A glance at the order of the meet of all N_q with $q \neq p$ leads us to the conclusion that this meet is equal to S_p. Thus S_p is a normal subgroup of G for each p, whence G is the direct sum of its Sylow-subgroups, in other words, G is nilpotent. This simple observation reduces the problem of determining all finite selfdual groups to the case of p-groups.

[2] The numbers in brackets refer to the Bibliography at the end of this paper.

so a representation

$$P_p = \sum C(p^\infty) + B_p$$

holds (since $\sum C(p^\infty)$ is, by a well-known theorem of BAER [1], a direct summand of every containing abelian group), where B_p is a reduced p-group, i. e., a p-group containing no subgroup of type $C(p^\infty)$.

The maximal number of linearly independent elements of infinite order in a group is called the *torsion free rank* of the group.

We shall denote the power of a group G by $|G|$.

§ 3. The countable abelian selfdual groups

All countable abelian selfdual groups are enumerated in the following

THEOREM 1. I. *A torsion free abelian group is never selfdual.*

II. *Among the countable abelian p-groups exactly those are selfdual which may be represented in the form*

(1) $$P_p = \sum_{k=1}^{\infty} C(p^{m_k}) \qquad (0 \leq m_k \leq m < \infty)$$

(the case of bounded groups), or in the form

(2) $$P_p = \sum_{\mathfrak{a}} C(p^\infty) + B_p$$

(the case of unbounded groups), where B_p is an arbitrary countable unbounded reduced p-group.

III. *Among the countable abelian torsion groups exactly those are selfdual every primary component of which is a group* (1) *or* (2).

IV. *Among the countable abelian mixed groups exactly those are selfdual which may be represented in the form*

(3) $$\sum_n C(\infty) + \sum_{p \text{ a prime}} P_p$$

(the case of finite torsion free rank) where n is an arbitrary natural number, P_p is an arbitrary p-group of type (2), *and the summation in the second term is extended over all primes p, or in the form*

(4) $$U + \sum_{\mathfrak{a}} (C + R + C(\infty))$$

(the case of infinite torsion free rank) where U is an arbitrary countable abelian group.

REMARKS. A finite abelian group is obviously always selfdual. This case is covered by statements II, III in the above theorem. — The standard manifold of the group P_p in (1) consists of all bounded abelian p-groups H for which the powers $|p^k H|$ do not exceed the corrresponding powers $|p^k P_p|$ for

$k=0, 1, \ldots$ — The standard manifold of (2) consists of all countable abelian p-groups. — The standard manifold of (3) consists of all abelian groups which are direct sums of an arbitrary countable abelian torsion group and of the direct sum of at most n infinite cyclic groups. — The standard manifold of (4) consists of all countable abelian groups.

PROOF OF THEOREM 1. Only statements II and IV require a proof. First we prove statement II. Since a bounded abelian p-group is a direct sum of cyclic groups of bounded order and such a group is obviously selfdual, we can restrict ourselves to the investigation of the *unbounded countable p-groups.*

We show that the group (2) is selfdual. Since every countable abelian p-group is a subgroup of

$$\sum_{\mathfrak{a}} C(p^\infty),$$

it is sufficient to prove that every countable abelian p-group is a homomorphic image of an arbitrary countable unbounded reduced group B_p. This follows immediately if we can show that B_p has a homomorphic image $\bar{B}_p$ such that *$\bar{B}_p$ is unbounded and $\bar{B}_p$ is a direct sum of cyclic groups.* In order to verify this, let us form the cross-cut (i. e. common part) D of all groups $B_p, pB_p, p^2B_p, \ldots, p^nB_p, \ldots$ Now we show that the group $B_p/D=\bar{B}_p$ has the required properties. As a matter of fact, since B_p is an unbounded reduced group, $p^{n+1}B_p$ is a proper subgroup of p^nB_p for each n. Hence B_p/D is an unbounded p-group. On the other hand, the group $B_p/D=\bar{B}_p$ contains no elements $\neq \bar{0}$ of infinite height; for if $\bar{b}=D+b$ is an element (= coset) of infinite height of $\bar{B}_p$, then the congruence $p^nx\equiv b \pmod D$ has a solution $x\in B_p$ for any natural number n, which implies $b\in p^nB_p$, i. e. $b\in D$, $\bar{b}=\bar{0}$. Thus, by a fundamental theorem of PRÜFER [2], $\bar{B}_p$ (as a countable abelian p-group without elements $\neq 0$ of infinite height) is a direct sum of cyclic groups. This completes the proof of our assertion that (2) is a selfdual group.

Now, let us assume, conversely, that P_p is a countable unbounded abelian selfdual group. We have to show that in this case the representation (2) holds. By forming in P_p the union A of all subgroups which are direct sums of groups $C(p^\infty)$, we get a representation

$$P_p=A+B_p \tag{5}$$

where

$$A=\sum C(p^\infty) \tag{6}$$

and B_p is a reduced p-group. We must still show that *the Σ on the right-hand side of* (6) *has an infinity of terms, and that in* (5) *B_p is an unbounded group.* We begin with the proof of the second assertion. Assume the contrary, i. e., that

$$p^mB_p=0 \tag{7}$$

for a suitable natural number m. Then we have by (5) and (6)

(8) $$p^{m+1}P_p = p^{m+1}A = A.$$

On the other hand, P_p (as an unbounded group) has a subgroup $C(p^{m+1})$ which is, by the selfdual property of P_p, at the same time a homomorphic image of P_p:

(9) $$P_p/K = C(p^{m+1}).$$

But then

(10) $$p^{m+1}P_p \subseteq K.$$

Hence, by (5), (8), (10) and (9), we have

$$B_p \cong P_p/A = P_p/p^{m+1}P_p \sim P_p/K = C(p^{m+1})$$

which contradicts (7). This contradiction proves that B_p *is an unbounded reduced countable abelian p-group*. Then, however, as we have seen in the preceding paragraph, every countable abelian p-group U is a homomorphic image of B_p, and consequently, a subgroup of P_p. Since this holds, in particular, for the group

$$U = \sum_{a} C(p^\infty),$$

A must have in the representation (6) *an infinity of terms* $C(p^\infty)$. This completes the proof of statement II in the theorem.

Now we are going to prove statement IV in our theorem. It is obvious that the groups (3) and (4) are selfdual. This follows immediately from the fact that an arbitrary countable abelian group is isomorphic to a subgroup of (4), and, on the other hand, it is a homomorphic image of

$$\sum_{a} C(\infty),$$

i. e., a fortiori of (4); furthermore, any subgroup of (3) is isomorphic to a direct sum of an arbitrary countable abelian torsion group and of the direct sum of at most n infinite cyclic groups, and exactly these groups exhaust all homomorphic images of (3).

Let us suppose, conversely, that G *is an arbitrary countable abelian selfdual mixed group*. First we consider the case in which *the torsion free rank n of G is finite*. We show that then G is a group of type (3). Let $a_1, \dots, a_n$ be a maximal independent system of elements of infinite order in G. These elements generate a subgroup S of G which is the direct sum of n infinite cyclic groups. Since S is, at the same time, a homomorphic image of G, we have the representation

(11) $$G = \{a_1'\} + \cdots + \{a_n'\} + T = \sum_{n} C(\infty) + T$$

where a_k' is an inverse image of a_k under a fixed homomorphism $G \sim S$, and T is the kernel of this homomorphism. From the fact that the torsion free rank of G is n, we infer by (11) that T is a torsion group.

Let p be an arbitrary prime number and P_p the p-primary component of T. Since G has obviously a homomorphic image $C(\infty)/pC(\infty)=C(p)$, the group P_p cannot be $=0$. We consider the representation of P_p in the form (5), (6) with a reduced p-group B_p, and we show that *B_p is an unbounded group.* As a matter of fact, if A in (5) and (6) contains but a finite number of direct summands $C(p^\infty)$, then the validity of our assertion follows from the fact that G has a homomorphic image of the form $C(\infty)/p^kC(\infty)+A=C(p^k)+A$ (see (11)) where k is an arbitrarily large natural number. Namely P_p must have also a subgroup $C(p^k)+A$, and so we infer from the finiteness of the members $C(p^\infty)$ in (6) that B_p is an unbounded group. — On the other hand, if A has an infinity of direct summands $C(p^\infty)$, then A contains an isomorphic copy of any countable abelian p-group as a subgroup. Consequently, any countable abelian p-group is a homomorphic image of G, i. e., also of

$$\sum_n C(\infty)+P_p=\sum_n C(\infty)+A+B_p \tag{12}$$

(see (11), (5), (6)). This, however, is impossible if B_p is bounded, since then every homomorphic image of (12) which is a p-group would be a direct sum of a group

$$\sum C(p^\infty)$$

and of a bounded group. Thus we have shown that *the subgroup B_p of P_p in* (5) *is an unbounded reduced group.* Then, however, as we have seen above, every countable abelian p-group is a homomorphic image of B_p, and consequently, a subgroup of P_p. Hence A in (6) *must have an infinity of direct summands* $C(p^\infty)$. Thus we have obtained that P_p is a group of type (2) which completes the present part of the proof.

Let G be, finally, *an arbitrary countable abelian selfdual mixed group the torsion free rank of which is infinite.* Then there exists an infinity of linearly independent elements of infinite order in G, and we get as before

$$G=\sum_a C(\infty)+M. \tag{13}$$

Since every countable abelian group is a homomorphic image of

$$\sum_a C(\infty)$$

and so, a fortiori, of G, we see that G contains an isomorphic copy of any countable abelian group as a subgroup. Thus G has a subgroup

$$L=\sum_a (C+R) \tag{14}$$

which must be contained even in the subgroup M of G. This follows from the fact that an arbitrary element of L is divisible by each natural number, while, by (13), no element of G not contained in M possesses this property.

On the other hand, L being a direct summand of any containing abelian group [1], we have

(15) $$M = L + U.$$

The representations (13), (15) and (14) show that G is a group (4) which completes the proof of our Theorem 1.

§ 4. The countable abelian dual groups

The following lemma, together with Theorem 1, will enable us to get a full oversight on all pairs of countable dual groups.

LEMMA. *Two arbitrary groups G and H are dual to each other if and only if they are selfdual and have the same standard manifold.*

The sufficiency of the stated condition is trivial, while its necessity will follow at once if we shall have established that the duality of G and H implies $S(G) = S(H)$. In order to verify the last equality, observe that G is a homomorphic image of itself and hence, by hypothesis, is isomorphic to a subgroup of H. Consequently, each subgroup of G is isomorphic to some subgroup of H, and conversely, q. e. d.

Now we formulate:

THEOREM 2. *Two countable abelian groups G and H are dual if and only if both of them are either p-groups, torsion groups or mixed groups, and besides:*

(i) (the case of p-groups) *they are bounded and $|p^k G| = |p^k H|$ holds for $k = 0, 1, 2, \ldots$, or they are of the form*

(16) $$G = G_p = \sum_{\alpha} C(p^\infty) + B_p, \quad H = H_p = \sum_{\alpha} C(p^\infty) + D_p$$

where B_p and D_p are arbitrary countable unbounded reduced p-groups;

(ii) (the case of torsion groups) *their p-primary components are dual for all primes p;*

(iii) (the case of mixed groups) *they are of the form*

$$G = \sum_{n} C(\infty) + \sum_{p \text{ a prime}} G_p, \quad H = \sum_{n} C(\infty) + \sum_{p \text{ a prime}} H_p$$

where G_p and H_p are groups having the form (16), *or are of the form*

$$G = U + \sum_{\alpha} (C + R + C(\infty)), \quad H = V + \sum_{\alpha} (C + R + C(\infty))$$

where U and V are arbitrary countable abelian groups.[3]

[3] It seems to be of some interest to note that all countable unbounded selfdual p-groups as well as all countable selfdual mixed groups of infinite torsion free rank are dual to each other.

Let us also mention the following corollary solving the problem as to which are the groups G with a dual pair.

COROLLARY. *A group G has a dual pair if and only if it is selfdual; H is a dual pair of G if and only if it is also selfdual with the same standard manifold.*

§ 5. The countable F—S-dual groups

The final problem with which we are concerned here is the characterization of all pairs of countable F—S-dual groups (and hence S—F-dual groups). Our result is the following

THEOREM 3. I. *If G and H are F—S-dual, then H is never torsion free; G and H are both p-groups, torsion groups or mixed groups, or else G is torsion free and H mixed.*

II. *The countable p-groups G_p and H_p are F—S-dual if and only if they are either bounded dual groups or are of the form*

$$G_p = \sum C(p^\infty) + B_p, \quad H_p = \sum_{\mathfrak{a}} C(p^\infty) + D_p \tag{17}$$

where B_p is a countable unbounded reduced p-group and D_p is an arbitrary countable p-group (the sum on the right member of (17_1) *contains a finite or a countable number of terms, eventually it may vanish).*

III. *The torsion groups G and H are F—S-dual if and only if all of their primary components G_p and H_p are F—S-dual.*

IV. *The countable mixed groups G and H are F—S-dual if and only if they have either the form*

$$G = \sum_n C(\infty) + \sum_{p \text{ a prime}} G_p, \quad H = \sum_n C(\infty) + \sum_{p \text{ a prime}} H_p \tag{18}$$

where n is any natural integer and for each p, the groups G_p and H_p are F—S-dual p-groups of type (17)*; or have the form*

$$G = U + \sum_{\mathfrak{a}} C(\infty), \quad H = V + \sum_{\mathfrak{a}} (R + C) \tag{19}$$

where U and V are arbitrary countable abelian groups.

The sufficiency of the conditions enumerated in this theorem follows immediately if we take into account that each (finite or) countable p-group resp. each (finite or) countable group is a homomorhic image of an arbitrary countable unbounded reduced p-group resp. of the group $\sum_{\mathfrak{a}} C(\infty)$, and is a subgroup of the group $\sum_{\mathfrak{a}} C(p^\infty)$ resp. of $\sum_{\mathfrak{a}} (R+C)$.

The proof of the necessity of I and III may clearly be omitted. Next let us suppose that G_p and H_p are two countable F—S-dual p-groups. We decompose G_p in the form

$$G_p = A + B_p = \sum C(p^\infty) + B_p$$

where A denotes the union of all subgroups of G_p which are direct sums of groups $C(p^\infty)$. If $A \neq 0$, then B_p is not bounded, for if $p^m B_p = 0$, then A being a homomorphic image of G, H contains a subgroup isomorphic to A, hence also one isomorphic to $C(p^{m+1})$, and the same inference as that used in the proof of Theorem 1 leads us to a contradiction. Therefore, either B_p is bounded and then $G_p = B_p$ is a bounded group implying the first alternative mentioned in II, or B_p is an unbounded reduced p-group and so it has a factorgroup isomorphic to $\sum_{\mathfrak{a}} C(p^\infty)$. In the latter case, by hypothesis, H_p must have the form (17_2).

Turning our attention to mixed groups, we first consider the case in which G has a finite torsion free rank n. Then H is of the same torsion free rank. Indeed, that the torsion free rank of H can not exceed n needs no verification, and since H must have a subgroup isomorphic to G/T (T is the torsion subgroup of G), it follows that the rank in question is exactly n. Defining the subgroup S of H as in § 3 before (11), we conclude that G has the form (11). Let W denote the torsion subgroup of H; hypothesis implies that G is homomorphic to H and hence to H/W. This factorgroup being a torsion free group of rank n, by (11) we obtain

$$H/W \cong G/T \cong \sum_n C(\infty)$$

whence

$$H = \sum_n C(\infty) + W = X + W.$$

The torsion subgroups T and W must be F—S-dual, for each homomorphic image of T is that of G and therefore it may be imbedded isomorphically in H and hence in W; on the other hand, if K is a subgroup of W, then $X + K$ is a subgroup of H and so a homomorphic image of G. A homomorphism $G \sim X + K$ preserves torsion free rank, consequently, the inverse image of K is just T, as desired. That all p-primary components of W are unbounded follows from the fact that $C(\infty)/p^k C(\infty)$ is a homomorphic image of G, for each natural k.

Finally, the case when G has an infinite torsion free rank is settled at once, considering that, by the same argument as that used in the case of finite torsion free rank, we arrive at the decomposition (19_1). But then G has a homomorphic image $\sum_{\mathfrak{n}} (R + C)$ which must be a subgroup and therefore also a direct summand of H. The proof of Theorem 3 is thus completed.

(Received 30 June 1953)

Bibliography

[1] R. Baer, The subgroup of the elements of finite order of an abelian group, *Ann. of Math. (Princeton)* (2), **37** (1936), pp. 766—781.

[2] H. Prüfer, Untersuchungen über die Zerlegbarkeit der abzählbaren primären Abelschen Gruppen, *Math. Z.*, **17** (1923), pp. 35—61.

[3] T. Szele, Ein Analogon der Körpertheorie für Abelsche Gruppen, *Journal f. d. reine u. angew. Math.*, **188** (1950), pp. 167—192.

ОБ ОДНОМ СПЕЦИАЛЬНОМ ВИДЕ ДВОЙСТВЕННОСТИ В ТЕОРИИ ГРУПП. I

Л. ФУКС (Будапешт), А. КЕРТЕС и Т. СЕЛЕ (Дебрецен)

(Резюме)

Группы G и H называются авторами S—F-двойственными, если многообразие всех подгрупп G — рассматриваемое как множество абстрактных групп — совпадает с многообразием всех факторгрупп от H. Группа G называется самодвойственной, если она S—F-двойственна самой себе. В настоящей работе дается явное определение всех счетных самодвойственных абелевых групп. — Получается следующий результат:

Группа без кручения не может быть самодвойственной. — Все самодвойственные p-группы задаются группами (1) и (2), где $C(r)$ означает циклическую группу порядка r $(1 \leqq r \leqq \infty)$, $C(p^\infty)$ будучи группой Прюфера типа (p^∞); в правой части (2) стоит прямая сумма счетного множества групп, а B_p есть любая счетная p-группа, не содержащая элемента наибольшего порядка и подгруппы типа $C(p^\infty)$. — Произвольная периодическая группа является самодвойственной тогда и только тогда, если всякий ее p-примарный компонент представляет собой группу типа (1) или (2). — Наконец из смешанных групп те и только те являются самодвойственными, которые допускают представление вида (3) или (4). В (3) стоит прямая сумма конечного числа бесконечных циклических групп, вторая же суммация распространяется на все простые числа, а P_p обозначает произвольную группу (2). В группе (4) R есть аддитивная группа сехв рациональных чисел, C — группа R взятая mod 1, а U — произвольная счетная абелева группа.

Кроме того авторы дают полное описание класса пар счетных абелевых групп S—F-двойственных между собой и пар групп, одна из которых S—F-двойственна другой.

GYULA SZŐKEFALVI-NAGY

1887—1953

C'est avec tristesse que nous faisons savoir la disparition d'un des membres du Comité de rédaction de nos Acta, le Professeur Gyula (Julius) Szőkefalvi-Nagy, membre de l'Académie des Sciences de Hongrie, mort le 14 octobre 1953 à Szeged. Il y a exercé comme professeur à la Faculté jusqu'au dernier jour, quoique fortement gêné pendant les dernières années de sa vie par son état de santé. Ses travaux mathématiques concernent principalement la géométrie algébrique, notamment la géométrie d'ordre fini de Juel, puis la répartition des zéros de polynomes et la théorie des constructions géométriques. Sur ce dernier sujet il a écrit une monographie en hongrois. C'était un travailleur enthousiaste, toujours entraîné par sa passion pour la science.

SUR LA SOMMABILITÉ DES SÉRIES ORTHOGONALES

Par

GEORGES ALEXITS (Budapest), membre de l'Académie

Introduction

Soit $\{\varphi_n(x)\}$ un système (non nécessairement complet) de fonctions orthogonales et normées dans l'intervalle fini (a, b). Désignons par

$$\sigma_n^{(\alpha)}(x) = \sum_{k=0}^{n} \frac{\binom{n-k+\alpha}{n-k}}{\binom{n+\alpha}{n}} c_k \varphi_k(x)$$

la n-ième moyenne (C, α) de la série orthogonale

$$c_0\varphi_0(x) + c_1\varphi_1(x) + \cdots + c_n\varphi_n(x) + \cdots \tag{1}$$

dont les coefficients $c_0, c_1, \ldots$ sont des nombres complexes arbitraires. Désignons ensuite par

$$K_n(t, x) = \sum_{k=0}^{n} \varphi_k(t)\varphi_k(x), \qquad K_n^{(1)}(t, x) = \frac{1}{n+1} \sum_{\nu=0}^{n} K_\nu(t, x)$$

les noyaux appartenants aux méthodes de sommation $(C, 0)$ et $(C, 1)$. Les fonctions de Lebesgue correspondantes sont

$$L_n(x) = \int_a^b |K_n(t, x)|\,dt, \qquad L_n^{(1)}(x) = \int_a^b |K_n^{(1)}(t, x)|\,dt.$$

Il est connu que les fonctions de Lebesgue $L_n^{(1)}(x)$ jouent un grand rôle dans la théorie de la sommation $(C, 1)$. En effet, S. KACZMARZ[1] a démontré que, si la série (1) est le développement d'une fonction $f \in L^2$, alors la condition $L_n^{(1)}(x) \leqq C$ pour $n = 0, 1, \ldots$ et $x \in E$ entraîne la sommabilité $(C, 1)$ de la série (1) sur E presque partout. Or on ne sait, s'il n'est pas suffisant que seulement certaines suites partielles $\{L_{\nu_n}(x)\}$ convenablement choisies des fonctions de Lebesgue appartenantes à la sommation $(C, 0)$ soient uniformément bornées pour assurer la sommabilité d'ordre $(C, \alpha > 0)$ de la série (1). Nous démontrerons à ce sujet le.

[1] S. KACZMARZ, Sur la convergence et la sommabilité des développements orthogonaux, *Studia Mathematica*, 1 (1929), p. 87—121.

THÉORÈME 1. *Si les fonctions de Lebesgue* $L_{2^n}(x)$ *d'ordre* 2^n *sont uniformément bornées sur un ensemble E et la condition*

$$\sum_{n=0}^{\infty} |c_n|^2 < \infty \tag{2}$$

est satisfaite, alors la série (1) *est pour tout* $\alpha > 0$ *sommable* (C, α) *sur l'ensemble E presque partout.*

Ce théorème donne lieu à des applications concernant la sommabilité de diverses séries orthogonales qui généralisent la série de WALSH.[2] Les fonctions orthogonales dont on forme les termes de ces séries s'obtiennent comme produits des fonctions de certains systèmes lacunaires, elles représentent donc en effet des généralisations du système de WALSH. On en déduit aisément une généralisation de la série de HAAR[3] avec les mêmes propriétés de sommabilité comme les séries généralisées de WALSH.

Quant à l'influence de l'ordre de grandeur des fonctions $L_n^{(1)}(x)$ sur la sommabilité des séries orthogonales, nous démontrerons le théorème mentionné de KACZMARZ dans la forme suivante:

THÉORÈME 4. *Si les fonctions de Lebesgue* $L_n^{(1)}(x)$ *sont uniformément bornées sur un ensemble E et la condition* (2) *est aussi satisfaite, alors la série* (1) *est pour tout* $\alpha > 0$ *sommable* (C, α) *sur E presque partout.*

La démonstration de ce théorème contient une solution d'une question posée par F. RIESZ[4] qui a proposé la tâche de démontrer la sommabilité $(C, 1)$ presque partout de la série de Fourier à coefficients satisfaisants à la condition (2) par des méthodes de la théorie des séries, sans faire appel à la fonction $f(x)$ elle-même dont la série est le développement de Fourier. La réponse à la question posée par F. RIESZ est contenue dans la démonstration du théorème 4.

En ce qui concerne la méthode de nos démonstrations, elle n'est pas neuve; une partie de l'idée principale remonte jusqu'à JEROSCH et WEYL;[5] elle était ensuite considérablement approfondie et complétée par KOLGOMOROV, SELIVERSTOV[6] et PLESSNER[7] dont le procédé d'évaluation des sommes parti-

[2] J. L. WALSH, A closed set of normal orthogonal functions, *American Journal of Mathematics*, **55** (1923), p. 5—24.

[3] A. HAAR, Zur Theorie der orthogonalen Funktionensysteme, *Thèse* (Göttingen, 1909), p. 37—48.

[4] F. RIESZ, Les ensembles de mesure nulle et leur rôle dans l'analyse, *Comptes Rendus du Premier Congrès des Mathématiciens Hongrois* (Budapest, 1952), p. 249.

[5] F. JEROSCH—H. WEYL, Über die Konvergenz von Reihen, die nach periodischen Funktionen fortschreiten, *Mathematische Annalen*, **64** (1909), p. 67—80.

[6] A. KOLMOGOROFF—G. SELIVERSTOFF, Sur la convergence des séries de Fourier, *Comptes Rendus Acad. Sci. Paris*, **178** (1925), p. 303—305 et *Rendiconti Acad. Lincei Roma*, **3** (1926), p. 307—310.

[7] A. PLESSNER, Über Konvergenz von trigonometrischen Reihen, *Journal f. reine u. angew. Mathematik*, **155** (1925), p. 15—25.

elles de la série de Fourier a été adapté par KACZMARZ[1] à l'évaluation des moyennes arithmétiques des séries orthogonales générales. Nos démonstrations suivent exactement les mêmes ordres d'idées, mais elles contiennent plusieures simplifications; à cause de cela, il nous semblait être plus convenable d'exposer les démonstrations in extenso que les interrompre par l'indication du lieu où se trouve l'un ou l'autre détail de la démonstration et de laisser ces détails aux soins du lecteur.

Démonstration du théorème 1

Nous montrons d'abord que, n_x étant une fonction mesurable qui ne prend que les valeurs $0, 1, \dots, n$, les intégrales de la forme

$$I_n = \int_a^b \Big[\int_E K_{2^{n_x}}(t, x)\,dx\Big]^2 dt$$

sont uniformément bornées. On a évidemment

$$I_n = \int_E\int_E\int_a^b K_{2^{n_x}}(t, x) K_{2^{n_y}}(t, y)\,dt\,dx\,dy. \tag{3}$$

Vu que les fonctions $\varphi_n(t)$ sont orthogonales et normées, il s'ensuit, en désignant par n_{xy} la plus petite des valeurs n_x et n_y:

$$\Big|\int_a^b K_{2^{n_x}}(t, x) K_{2^{n_y}}(t, y)\,dt\Big| = |K_{2^{n_{xy}}}(x, y)| \leqq |K_{2^{n_x}}(x, y)| + |K_{2^{n_y}}(x, y)|.$$

D'après l'hypothèse, on a pour tout $x \in E$

$$L_{2^{n_x}}(x) = \int_a^b \big|K_{2^{n_x}}(x, y)\big|\,dy \leqq C.$$

Il s'ensuit donc en vertu de (3):

$$I_n \leqq \int_E\int_E \big|K_{2^{n_x}}(x, y)\big|\,dx\,dy + \int_E\int_E \big|K_{2^{n_y}}(x, y)\big|\,dx\,dy \leqq 2C|E| \tag{4}$$

où $|E|$ désigne la mesure de l'ensemble E; ce qui était justement notre assertion concernant l'ordre de grandeur des intégrales I_n.

Remarquons maintenant qu'en profitant de la condition (2), on peut aisément construire une suite $\{\lambda_n\}$ de nombres positifs tels que

$$A = \sum_{n=0}^{\infty} |c_n|^2 \lambda_n^2 < \infty \tag{5}$$

où $\{\lambda_n^{-1}\}$ est une suite convexe tendant vers zéro. Désignons par $s_n^*(x)$ la n-ième somme partielle de la série $\sum c_n \lambda_n \varphi_n(x)$ et soit n_x le plus petit indice pour lequel

$$s_{2^{n_x}}^*(x) = \operatorname*{Max}_{\nu \leqq n} s_{2^\nu}(x).$$

La suite $\{s^*_{2^{n_x}}(x)\}$ étant non-décroissante, elle a une fonction-limite $s^*(x)$ et on a évidemment

(6) $$s^*(x) \geqq s^*_{2^n}(x) \qquad (n=0,1,\ldots).$$

Mais on obtient d'après (4) et (5):

$$\int_E s^*_{2^{n_x}}(x)\,dx \leqq \left|\int_E \int_a^b s^*_{2^n}(t) K_{2^{n_x}}(t,x)\,dt\,dx\right| \leqq$$

$$\leqq \left\{\int_a^b \left[s^*_{2^n}(t)\right]^2 dt \int_a^b \left[\int_E K_{2^{n_x}}(t,x)\,dx\right]^2 dt\right\}^{\frac{1}{2}} \leqq \sqrt{2AC|E|}.$$

Il s'ensuit donc grâce à un théorème connu de B. Levi que

$$\int_E s^*(x)\,dx \leqq \sqrt{2AC|E|};$$

par conséquent $s^*(x)$ est une fonction presque partout finie sur l'ensemble E d'où il résulte d'après (6) que les sommes partielles $s^*_{2^n}(x)$ sont bornées supérieurement par $s^*(x)$ pour presque tous les $x \in E$. En répétant ce raisonnement appliqué à la suite $\{-s^*_{2^n}(x)\}$, on obtient qu'elle est aussi uniformément bornée supérieurement pour presque tous les $x \in E$; c'est à dire que la suite $\{|s^*_{2^n}(x)|\}$ est uniformément bornée sur E presque partout. Désignons par $\sigma^*_n(x)$ la n-ième moyenne arithmétique de la série $\Sigma c_n \lambda_n \varphi_n(x)$. Kolmogorov[8] a démontré qu'en conséquence de (5), la différence $s^*_{2^n}(x) - \sigma^*_{2^n}(x)$ converge presque partout vers zéro, les moyennes arithmétiques $\sigma^*_{2^n}(x)$ sont donc aussi uniformément bornées sur E presque partout. De plus, Kaczmarz[9] a démontré que, m étant un indice arbitraire compris entre 2^n et 2^{n+1}, la différence $\sigma^*_m(x) - \sigma^*_{2^n}(x)$ tend, sous la condition (5), presque partout vers zéro. Toutes les moyennes arithmétiques $\sigma^*_n(x)$ sont donc uniformément bornées sur E presque partout. Puisque

$$\sum_{n=0}^{\infty} c_n \varphi_n(x) = \sum_{n=0}^{\infty} \frac{1}{\lambda_n} c_n \lambda_n \varphi_n(x),$$

et les $\sigma^*_n(x)$ sont bornées dans leur ensemble sur E presque partout, il en résulte d'après un théorème[10] concernant les séries de fonctions arbitraires que les moyennes arithmétiques $\sigma^{(1)}_n(x)$ de la série $\Sigma c_n \varphi_n(x)$ sont presque partout convergentes sur l'ensemble E, ce qui équivaut, grâce à un

[8] A. Kolmogoroff, Une contribution à l'étude de la convergence des séries de Fourier, *Fundamenta Mathematicae*, 5 (1924), p. 96—97.

[9] S. Kaczmarz, Über die Reihen von allgemeinen Orthogonalfunktionen, *Mathematische Annalen*, 96 (1925), p. 148—151.

[10] Voir p. ex. G. Alexits, Über die Transformierten der arithmetischen Mittel von Orthogonalreihen, *Acta Mathematica Acad. Sci. Hung.*, 2 (1951), p. 1—8.

théorème de ZYGMUND,[11] à la sommabilité (C, α) pour tout $\alpha > 0$ sur E presque partout.

Sommabilité des séries de Walsh et de Haar généralisées

Appelons un système de fonctions $\{\psi_n(x)\}$ multiplement orthogonal et normé, si pour toute combinaison d'indices $\nu_1, \nu_2, \ldots, \nu_p$ qui n'est pas constituée d'exactement $p/2$ paires d'indices égaux on a

$$\int_a^b \psi_{\nu_1}(x)\psi_{\nu_2}(x)\ldots\psi_{\nu_p}(x)dx = 0,$$

tandis que

$$\int_a^b \psi^2_{\nu_1}(x)\psi^2_{\nu_2}(x)\ldots\psi^2_{\nu_p}(x)dx = 1.$$

Tels sont par exemple les systèmes de fonctions normées indépendantes au sens stochastique. Mentionnons à titre d'exemples concrets : le système $\{r_n(x)\}$ des fonctions de RADEMACHER,[12] puis le système $\{e^{2\pi i \vartheta_n(x)}\}$ dû à STEINHAUS[13] où $\vartheta_n(x)$ est défini de la manière suivante : Soit $0, \xi_1\xi_2\ldots$ le développement dyadique infini du nombre positif $x \leqq 1$, alors

$$\vartheta_1(x) = 0, \xi_1\xi_3\xi_6\,\xi_{10}\ldots,$$
$$\vartheta_2(x) = 0, \xi_2\xi_5\xi_9\,\xi_{14}\ldots,$$
$$\vartheta_3(x) = 0, \xi_4\xi_8\xi_{13}\xi_{19}\ldots,$$
$$\cdots\cdots\cdots\cdots$$

Tous ces systèmes sont multiplicativement orthogonaux et normés dans l'intervalle $(0, 1)$. Bornons nous à cet intervalle ; nous appellerons le système $\{\varphi_n(x)\}$ de fonctions définies par $\varphi_0(x) \equiv 1$ et

$$\varphi_n(x) = \psi_{\nu_1}(x)\psi_{\nu_2}(x)\ldots\psi_{\nu_p}(x) \qquad (1 \leqq \nu_1 < \nu_2 < \ldots < \nu_p)$$

pour $n = 2^{\nu_1} + 2^{\nu_2} + \cdots + 2^{\nu_p}$, système de WALSH généralisé engendré par le système multiplicativement orthogonal et normé $\{\psi_n(x)\}$. Les fonctions $\varphi_n(x)$ sont évidemment elles-mêmes orthogonales et normées. Quant à leur noyau $K_{2^n}(t, x)$, on voit immédiatement que

$$K_{2^n}(t, x) = \prod_{k=1}^{n} (1 + \psi_k(t)\psi_k(x)).$$

Si les fonctions $|\psi_n(x)|$ ont 1 comme borne commune, on obtient donc

$$K_{2^n}(t, x) \geqq 0.$$

[11] A. ZYGMUND, Sur l'application de la première moyenne arithmétique dans la théorie des séries de fonctions orthogonales, *Fundamenta Mathematicae*, **10** (1927), p. 356—362.

[12] H. RADEMACHER, Einige Sätze über Reihen von allgemeinen Orthogonalfunktionen, *Mathematische Annalen*, **87** (1922), p. 112—138.

[13] H. STEINHAUS, Sur la probabilité de la convergence de séries, *Studia Mathematica*, **2** (1930), p. 21—39.

Or les fonctions $\varphi_n(x)$ étant orthogonales à la fonction $\varphi_0(x)\equiv 1$, les fonctions de Lebesgue d'ordre 2^n se calculent par la relation

$$L_{2^n}(x)=\int_0^1 K_{2^n}(t,x)\,dt=\varphi_0(x)\int_0^1\varphi_0(t)\,dt=1.$$

En appliquant donc notre théorème 1, nous obtenons le

Théorème 2. *Si les fonctions $\{\psi_n(x)\}$ sont soumises à la condition $|\psi_n(x)|\leqq 1$ et les nombres complexes $c_0, c_1, \ldots$ satisfont à la condition* (2), *alors la série de* Walsh *généralisée $\Sigma c_n\varphi_n(x)$ engendrée par le système $\{\psi_n(x)\}$ est presque partout sommable (C,α) pour tout $\alpha>0$.*

Définissons maintenant un système $\{\chi_n^{(k)}(x)\}$ où $1\leqq k\leqq 2^{n-1}$ comme suit:

$$\chi_0^{(0)}(x)\equiv 1,\quad \chi_1^{(1)}(x)=\varphi_1(x)$$

et pour $n=2$:

$$\chi_2^{(1)}(x)=\frac{1}{\sqrt{2}}[\varphi_2(x)+\varphi_3(x)],$$

$$\chi_2^{(2)}(x)=\frac{1}{\sqrt{2}}[\varphi_2(x)-\varphi_3(x)].$$

Pour $n\geqq 3$ on construit $\chi_n^{(k)}(x)$ inductivement: soit $\alpha_{k\nu}^{(n-1)}=\pm 1$ le coefficient de la fonction $\varphi_\nu(x)$ dans la relation

$$\chi_{n-1}^{(k)}(x)=\frac{1}{\sqrt{2^{n-2}}}\sum_{\nu=2^{n-2}}^{2^{n-1}-1}\alpha_{k\nu}^{(n-1)}\varphi_\nu(x).$$

Construisons maintenant la matrice $\|\alpha_\nu^{(n)}\|$ en écrivant deux fois chaque ligne de la matrice $\|\alpha_\nu^{(n-1)}\|$ et en la complétant par répétition de la même ligne, une fois sans changement, la deuxième fois avec des signes contraires. On définit alors[11]

$$\chi_n^{(k)}(x)=\frac{1}{\sqrt{2^{n-1}}}\sum_{\nu=2^{n-1}}^{2^n-1}\alpha_{k\nu}^{(n)}\varphi_\nu(x).$$

Dans le cas où $\{\varphi_n(x)\}$ est un système généralisé de Walsh, nous appellerons $\{\chi_n^{(k)}(x)\}$ le système généralisé de Haar engendré par le système $\{\varphi_n(x)\}$. (Dans le cas où $\{\varphi_n(x)\}$ est le système de Walsh engendré par le système de Rademacher, on obtient pour $\{\chi_n^{(k)}(x)\}$ le système de Haar proprement dit.) Envisageons la série

$$\sum_{n=0}^{\infty} c_n\chi_n^{(k)}(x) \tag{7}$$

[11] Cette construction est due à S. Kaczmarz, Über ein Orthogonalsystem, *Comptes Rendus I. Congrès des Pays Slaves* (Warszawa, 1929), p. 189—192.

en supposant que les coefficients c_n sont réels et soumis à la condition (2). Alors, le théorème de RIESZ—FISCHER assure l'existence d'une fonction $f \in L^2$ dont (7) est le développement de HAAR généralisé. Désignons par $h_n(x)$ la n-ième somme partielle de (7) et par $w_n(x)$ la n-ième somme partielle du développement de la même fonction $f(x)$ suivant le système de WALSH généralisé $\{\varphi_n(x)\}$ correspondant au système $\{\chi_n^{(k)}(x)\}$. KACZMARZ a montré[14] que

$$h_{2^n}(x) \equiv w_{2^n}(x).$$

Mais $f \in L^2$ entraîne, grâce au théorème 2, la sommabilité (C, α) presque partout de son développement suivant le système $\{\varphi_n(x)\}$. Il s'ensuit d'après KOLMOGOROV[8] que la suite $\{w_{2^n}(x)\}$ converge presque partout, par conséquent $\{h_{2^n}(x)\}$ est aussi presque partout convergent; ce qui entraîne, grâce aux théorèmes de KACZMARZ[9] et de ZYGMUND,[11] la sommabilité (C, α) presque partout du développement de $f(x)$ suivant le système $\{\chi_n^{(k)}(x)\}$. Ainsi, nous avons obtenu le

THÉORÈME 3. *Le développement d'une fonction $f \in L^2$ en série de* HAAR *généralisée est presque partout sommable* (C, α) *pour tout* $\alpha > 0$.

Si $\{\chi_n^{(k)}(x)\}$ est le système de HAAR proprement dit, notre théorème n'atteint pas la généralité du théorème de HAAR[3] d'après lequel même les développements des fonctions $f \in L$ sont presque partout convergents.

Démonstration du théorème 4

Retournons aux systèmes généraux de fonctions orthogonales et normées dans un intervalle fini (a, b). Pour démontrer le théorème 4, il ne nous faut que l'évaluation des intégrales de la forme

$$J_n = \int_E \int_E \int_a^b K_{n_x}^{(1)}(t, x) K_{n_y}^{(1)}(t, y)\, dt\, dx\, dy$$

sous la condition $L_n^{(1)}(x) \leq C$ pour $x \in E$. Vu que

$$K_m^{(1)}(t, x) = \frac{\sum_{\nu=0}^{m} K_\nu(t, x)}{m+1},$$

on obtient pour un couple de valeurs x, y avec $n_x \leq n_y$, en tenant compte de l'orthogonalité des fonctions $\varphi_n(x)$:

$$\int_a^b K_{n_x}^{(1)}(t, x) K_{n_y}^{(1)}(t, y)\, dt = \frac{\sum_{\nu=0}^{n_x} K_\nu(x, y)(n_y + 1 - \nu)}{(n_x + 1)(n_y + 1)}.$$

En écrivant donc $n_x + 1 + n_y - n_x - 1$ au lieu de n_y, le deuxième membre

peut être écrit dans la forme

$$\frac{1}{n_y+1}\sum_{\nu=0}^{n_x}\left(1-\frac{\nu}{n_x+1}\right)K_\nu(x,y)+\frac{n_y-n_x}{n_y+1}\,\frac{\sum\limits_{\nu=0}^{n_x}K_\nu(x,y)}{n_x+1}=$$

$$=\frac{\sum\limits_{\nu=0}^{n_x}(\nu+1)K_\nu^{(1)}(x,y)}{(n_x+1)(n_y+1)}+\frac{n_y-n_x}{n_y+1}K_{n_x}^{(1)}(x,y).$$

Par conséquent, on obtient pour $n_x \leqq n_y$

$$\left|\int_a^b K_{n_x}^{(1)}(t,x)K_{n_y}^{(1)}(t,y)\,dt\right| \leqq \frac{\sum\limits_{\nu=0}^{n_x}|K_\nu^{(1)}(x,y)|}{n_x+1}+|K_{n_x}^{(1)}(x,y)|$$

et une relation analogue est valable, en échangeant x et y, pour un couple de valeurs x, y avec $n_x > n_y$. Il en résulte, vu que $L_{n_x}^{(1)}(x) \leqq C$ et $L_{n_y}^{(1)}(y) \leqq C$ pour tout $x, y \in E$,

$$J_n \leqq 2\int_E\int_E \frac{\sum\limits_{\nu=0}^{n_x}|K_\nu^{(1)}(x,y)|}{n_x+1}\,dx\,dy+2\int_E\int_E|K_{n_x}^{(1)}(x,y)|\,dx\,dy \leqq 4C\int_E dx = 4C|E|.$$

Envisageons de nouveau la série $\Sigma c_k\lambda_k\varphi_k(x)$ et nous obtenons pour l'intégrale de $\sigma_{n_x}^*(x)$:

$$\int_E \sigma_{n_x}^*(x)\,dx \leqq \left|\int_E\int_a^b s_n(x)K_{n_x}^{(1)}(t,x)\,dt\,dx\right| \leqq 2\sqrt{AC|E|}.$$

On en déduit d'une manière tout à fait analogue comme dans le cas des sommes partielles $s_{2^n}^*(x)$ que les moyennes arithmétiques $\sigma_n^*(x)$ sont uniformément bornées sur E presque partout. Ce fait entraîne,[10] la convergence de la suite $\{\sigma_n^{(1)}(x)\}$ sur l'ensemble E presque partout, ce qui équivaut[11] à la convergence sur E presque partout de la suite $\{\sigma_n^{(\alpha)}(x)\}$ pour tout $\alpha > 0$.

(Reçu le 31 auguste 1953.)

О СУММИРУЕМОСТИ ОРТОГОНАЛЬНЫХ РЯДОВ

Г. АЛЕКСИЧ (Будапешт)

(Резюме)

Пусть $\{\varphi_n(x)\}$ произвольная (необъязательно полная) ортонормальная система функций, заданная на конечном отрезке (a, b). Обозначим через

$$K_n(t, x) = \sum_{k=0}^{n} \varphi_k(t)\,\varphi_k(x), \qquad K_n^{(1)}(t, x) = \frac{1}{n+1} \sum_{k=0}^{n} K_k(t, x)$$

ядра, относящиеся к $(C, 0)$-, соответственно $(C, 1)$-суммированию ортогонального ряда

$$\sum_{n=0}^{\infty} c_n \varphi_n(x), \tag{1}$$

и через

$$L_n(x) = \int_a^b |K_n(t, x)|\, dt, \qquad L_n^{(1)}(x) = \int_a^b |K_n^{(1)}(t, x)|\, dt$$

соответствующие функции Лебега.

Используя идею, с помощью которой Колмогоров, Селиверстов и Плеснер доказали свою известную теорему о сходимости рядов Фурье, получаем следующие результаты:

Если последовательность $\{L_{2^n}(x)\}$ равномерно ограничена на множестве E и

$$\sum_{n=0}^{\infty} |c_n|^2 < \infty, \tag{2}$$

тогда ряд (1) является (C, α)-суммируемым почти всюду на множестве E, если только $\alpha > 0$.

В качестве применения этой теоремы получается обобщение ортогональных рядов Хаара и Уэлша, обладающис тем своиствам, что полученный ряд будет (C, α)-суммируемым $(\alpha > 0)$ почти всюду, если выполняется (2). Этот результат перекрывает результаты Качмаржа и Пели, относящиеся к суммированию обыкновенного ряда Уэлша.

Наконец дается простое доказательство следующией теоремы Качмаржа:

Если последовательность $\{L_n^{(1)}(x)\}$ равномерно ограничена на множестве E и выполняется (2), тогда ряд (1) является (C, α)-суммируемым почти всюду на множестве E, если только $\alpha > 0$.

Приведенное доказательство не только проще, чем первоначальное доказательство Качмаржа, но кроме того оно опирается только на условие (2) и на средств теории рядов, без привлечения функции $f(x) + ig(x)$ для которой (1) является вследствие (2) и на основе теоремы Рисса—Фишера рядом Фурье относительно системы $\{\varphi_n(x)\}$. Тем самым мы решили также проблему Ф. Рисса, возникшую в связи с некоторым тригонометрическим рядом Фурье.

ON THE THEORY OF ORDER STATISTICS

By

ALFRÉD RÉNYI (Budapest), corresponding member of the Academy

Dedicated to A. N. KOLMOGOROV
on the occasion of his 50th birthday

Introduction

Since the beginning of the century many authors, e. g. K. PEARSON [1], L. v. BORTKIEWICZ [2], E. L. DODD [3], L. H. C. TIPPET [4], and M. FRÉCHET [5] have dealt with particular problems which may be classified as belonging to the theory of order statistics. A. N. KOLMOGOROV [6], V. I. GLIVENKO [7], N. V. SMIRNOV [8], B. V. GNEDENKO [9], and other mathematicians having recognized the great theoretical and practical importance of this set of problems, developed this subject into a systematical theory.

In the last three years a particularly great number of papers dealt with such problems; of these we mention those of B. V. GNEDENKO and V. S. KOROLUK [10], B. V. GNEDENKO and E. L. RVAČEVA [11], B. V. GNEDENKO and V. S. MIHALEVIČ [12], V. S. MIHALEVIČ [13], J. D. KVIT [14], G. M. MANIA [15], I. I. GIHMAN [16], W. FELLER [17], J. L. DOOB [18], F. J. MASSEY [19], M. D. DONSKER [20], T. W. ANDERSON and D. A. DARLING [21]. A bibliography up to 1947 is to be found in the paper of S. S. WILKS [30] enumerating 90 papers.

The purpose of the present paper is to give a new method by means of which many important results of the theory of order statistics can be obtained with surprising simplicity; the method also enables us to prove several new theorems. The essential novelty of this method is that it reduces the problems connected with order statistics to the study of sums of mutually independent random variables. § 1 contains the review of the method, § 2 is devoted to the proof of some known theorems by means of this method, and § 3 contains the formulation of some new results obtained by this method, concerning the comparison of the sample distribution function to that of the population. These results are connected with the fundamental results of A. N. KOLMOGOROV and N. V. SMIRNOV.

Let $F_n(x)$ denote the distribution function of a sample of size n drawn from a population having the continuous distribution function $F(x)$, in other

words, $F_n(x)$ denotes the frequency ratio of sample values not exceeding x. KOLMOGOROV determined the limiting distribution of the supremum of $|F_n(x)-F(x)|$, SMIRNOV did the same for $F_n(x)-F(x)$; in § 4 we shall determine the limiting distribution of the supremum* of the relative deviations $\frac{F_n(x)-F(x)}{F(x)}$, and $\left|\frac{F_n(x)-F(x)}{F(x)}\right|$, respectively. To do this, besides our method, the lemmas in § 4, generalizing some results of P. ERDŐS and M. KAC [22], are needed. These lemmas are of certain interest in themselves. § 5 contains the proof of the results formulated in § 3, while § 6 contains some remarks on the numerical computation of the values of the limiting distribution functions occurring in our theorems; tables for one of these are also given. I have found the method formulated in § 1 by analysing a theorem of S. MALMQUIST [23]; § 1 contains among others a new and simple proof for this theorem of MALMQUIST. Together with G. HAJÓS, we have found another simple proof of this theorem which will be published in a joint paper of ours [24]. All these investigations have for their origin in the discussions in a seminary of the Departments of Probability Theory and of Mathematical Statistics of the Institute for Applied Mathematics of the Hungarian Academy of Sciences. I lectured on the part of the results contained in this paper in January 1953 on the congress of the Humboldt University in Berlin[1] and in September 1953 on the VIIIth Polish Mathematical Congress in Warsaw. On this last occasion A. N. KOLMOGOROV has made certain valuable remarks for which I express him my most sincere thanks. Further, I express my thanks to T. LIPTÁK who participated in the preparation of this paper by elaboration of some particular calculations, as well as to Miss I. PALÁSTI and Mrs. P. VÁRNAI for the numerical computations.

§ 1. A new method in the theory of order statistics

Let us start with the following special case: let a sample of size n be given concerning the value of a random variable ζ of exponential distribution, i. e. the results of n independent observations for its value, denoted by $\zeta_1, \zeta_2, \ldots, \zeta_n$; in other words, $\zeta_1, \zeta_2, \ldots, \zeta_n$ are mutually independent random variables with the same distribution function of exponential type. We need the following well-known property of the exponential distribution: if ζ is an exponentially distributed random variable, then

$$\mathbf{P}(\zeta < x+y \mid \zeta \geqq y) = \mathbf{P}(\zeta < x), \tag{1.1}$$

* (in an interval $0 < a \leqq F(x) \leqq b \leqq 1$).

[1] This lecture will be published in the communications of the Congress under the following title: "Eine neue Methode in der Theorie der geordneten Stichproben".

if $x > 0$ and $y \geqq 0$.[2] This property characterizes uniquely the exponential distribution. Indeed, let $F(x)$ be the distribution function of ζ, then

$$\mathbf{P}(\zeta < x + y \mid \zeta \geqq y) = \frac{F(x+y) - F(y)}{1 - F(y)}$$

and it follows that (1. 1) is equivalent to the following relation:

$$\Phi(x+y) = \Phi(x)\Phi(y) \tag{1.2}$$

where $\Phi(x) = 1 - F(x)$. It is known however that, of all functions satisfying the condition $0 \leqq \Phi(x) \leqq 1$, except for the trivial cases $\Phi(x) \equiv 0$ and $\Phi(x) \equiv 1$, the functions $\Phi(x) = e^{-\lambda x}$ $(\lambda > 0)$ and only these satisfy the functional equation (1. 2).

The meaning of (1. 1) becomes especially clear, if the random variable ζ is interpreted as the duration of a happening having random duration. In this interpretation the proposition (1. 1) can be formulated as follows: in case of a happening of exponentially distributed random duration, being in progress at the moment y, the further duration of the happening does not depend on y, i. e. on its duration until the given moment.

Let us arrange the numbers $\zeta_1, \zeta_2, \ldots, \zeta_n$ in order of magnitude and use the notation

$$\zeta_k^* = R_k(\zeta_1, \zeta_2, \ldots, \zeta_n) \qquad (k = 1, 2, \ldots, n) \tag{1.3}$$

where the function $R_k(x_1, x_2, \ldots, x_n)$ of the n variables $x_1, x_2, \ldots, x_n$ denotes the k-th of the values $x_1, x_2, \ldots, x_n$ in order of magnitude $(k = 1, 2, \ldots, n)$; thus e. g. $\zeta_1^* = \min_{1 \leqq k \leqq n} \zeta_k$ and $\zeta_n^* = \max_{1 \leqq k \leqq n} \zeta_k$. Then the individual and joint distributions of the values of the *order statistics* $\zeta_1^* \leqq \zeta_2^* \leqq \cdots \leqq \zeta_n^*$ can be most easily determined. For that purpose we interpret the variables ζ_k as random durations of mutually independent happenings; then ζ_k^* denotes the duration of the happening finished as k-th of the n happenings. Let us determine, first of all, the distributions of the differences $\zeta_{k+1}^* - \zeta_k^*$. If $\zeta_k^* = y$, then

$$\mathbf{P}(\zeta_{k+1}^* - \zeta_k^* > x \mid \zeta_k^* = y) = \mathbf{P}(\zeta_{k+1}^* > x + y \mid \zeta_k^* = y) \tag{1.4}$$

where on the right side there stands the probability of the event that none of the $n-k$ happenings, being in progress at the moment y, finishes until the moment $x+y$. By virtue of (1. 1), the value of this probability is

$$(\mathbf{P}(\zeta > x))^{n-k} = e^{-(n-k)\lambda x}$$

and thus the conditional distribution function of $\zeta_{k+1}^* - \zeta_k^*$ with respect to the condition $\zeta_k^* = y$ is

$$\mathbf{P}(\zeta_{k+1}^* - \zeta_k^* < x \mid \zeta_k^* = y) = 1 - e^{-(n-k)\lambda x}. \tag{1.5}$$

[2] $\mathbf{P}(A)$ denotes the probability of the event A, and $\mathbf{P}(A \mid B)$ denotes the conditional probability of the event A with respect to the event B.

As the conditional distribution function (1.5) does not depend on y, (1.5) gives also the non-conditional distribution function of $\zeta_{k+1}^* - \zeta_k^*$; indeed, by virtue of the theorem on total probability,

$$(1.6) \qquad \mathbf{P}(\zeta_{k+1}^* - \zeta_k^* < x) = \int_0^\infty \mathbf{P}(\zeta_{k+1}^* - \zeta_k^* < x \mid \zeta_k^* = y) d\mathbf{P}(\zeta_k^* < y) = 1 - e^{-(n-k)\lambda x}.$$

Therefore the differences $\zeta_{k+1}^* - \zeta_k^*$ are themselves exponentially distributed with the mean value $\frac{1}{(n-k)\lambda}$ and thus the variables

$$(1.7) \qquad \delta_{k+1} = (n-k)\,(\zeta_{k+1}^* - \zeta_k^*) \qquad (k = 0, 1, \ldots, n-1)$$

are also exponentially distributed with the mean value $\frac{1}{\lambda}$. (In the above relation by definition $\zeta_0^* \equiv 0$.)

It follows from the abovesaid that the variables $\delta_1, \delta_2, \ldots, \delta_n$ are mutually independent random variables. It is namely easy to see that the probability

$$(1.8) \qquad \mathbf{P}(\zeta_{k+1}^* - \zeta_k^* < x \mid \zeta_1^* = y_1, \zeta_2^* - \zeta_1^* = y_2, \ldots, \zeta_k^* - \zeta_{k-1}^* = y_k)$$

does not depend on the variables $y_1, y_2, \ldots, y_k$; this is evident, as the above conditions mean that $\zeta_1^* = y_1, \zeta_2^* = y_1 + y_2, \ldots, \zeta_k^* = y_1 + y_2 + \cdots + y_k$; i. e. they give the moments of the finishing of k happenings, which finish first of the n happenings which started simultaneously at the moment $t = 0$. These conditions imply that at the moment $t = y_1 + y_2 + \cdots + y_k$ there are still $n-k$ happenings in progress and the probability of the finishing of at least one of them before the moment $t + x$ is equal to $1 - e^{-(n-k)\lambda x}$. Thus the probability of the left hand side of (1.8) equals $1 - e^{-(n-k)\lambda x}$, i. e. it does not depend on the variables $y_1, y_2, \ldots, y_k$, and this is equivalent to the fact that the variables $\zeta_{k+1}^* - \zeta_k^*$ (and also the variables δ_k) are mutually independent. Thus the variables ζ_k^* can be expressed in the form

$$(1.9) \qquad \zeta_k^* = \frac{\delta_1}{n} + \frac{\delta_2}{n-1} + \cdots + \frac{\delta_k}{n-k+1} \qquad (k = 1, 2, \ldots, n)$$

i. e. as linear forms of mutually independent random variables having the same distribution. (1.9) can be also expressed by saying that *the variables ζ_k^* form an (additive) Markov chain.* By virtue of (1.9) the distribution of any ζ_k^*, further, the joint distribution of any number of the variables ζ_k^* can be determined in explicit form.

Consider now, how the abovesaid can be applied in general to the study of order statistics. Let ξ be any random variable having a continuous and steadily increasing[3] distribution function $F(x)$, let $(\xi_1, \xi_2, \ldots, \xi_n)$ be a

[3] By saying that $F(x)$ is steadily increasing, we mean that $F(x)$ is a strictly increasing monotone function in the least interval (a, b) where $F(a) = 0$ and $F(b) = 1$; it may be happen that $a = -\infty$ or $b = +\infty$.

sample of size n consisting of n independent observations of the value of ξ, that is to say, let $\xi_1, \xi_2, \dots, \xi_n$ be mutually independent random variables with the same (continuous) distribution function $F(x)$. Let us arrange the sample values ξ_k in order of magnitude, that is to say, let us form the new variables $\xi_k^* = R_k(\xi_1, \xi_2, \dots, \xi_n)$.

The main problem of order statistics is to study the variables ξ_k^*; this, however, can be reduced to the special case when the variables ξ_k are exponentially distributed (and therefore — by virtue of (1.9) — to the study of sums of mutually independent random variables), as follows: let us put

$$\eta_k = F(\xi_k) \quad \text{and} \quad \zeta_k = \log \frac{1}{\eta_k} \qquad (k = 1, 2, \dots, n) \tag{1.10}$$

and let us denote by $\eta_k^* = F(\xi_k^*)$ the k-th of the variables $\eta_1, \eta_2, \dots, \eta_n$ in order of magnitude, i. e. let us put $\eta_k^* = R_k(\eta_1, \eta_2, \dots, \eta_n)$; further, let us put

$$\zeta_k^* = \log \frac{1}{\eta_{n+1-k}^*} \qquad (k = 1, 2, \dots, n). \tag{1.11}$$

As $\log \frac{1}{x}$ is a steadily decreasing function, we obtain:

$$\zeta_k^* = R_k(\zeta_1, \zeta_2, \dots, \zeta_n) \qquad (k = 1, 2, \dots, n), \tag{1.12}$$

whence ζ_k^* is the k-th of the variables $\zeta_1, \zeta_2, \dots, \zeta_n$ in order of magnitude. As we have assumed the variables ξ_k to be mutually independent, it follows that the variables ζ_k are also mutually independent.

Let us investigate now the distribution of the single variable ζ_k. $F(x)$ being a strictly increasing function, the inverse function of $x = F(y)$, denoted by $y = F^{-1}(x)$, is uniquely defined in the interval $0 \leqq x \leqq 1$, and thus

$$\mathbf{P}(\zeta_k < x) = \mathbf{P}\left(\log \frac{1}{F(\zeta_k)} < x\right) = \mathbf{P}(\xi_k > F^{-1}(e^{-x})) = 1 - F(F^{-1}(e^{-x})) = 1 - e^{-x},$$

if $0 \leqq x \leqq 1$. Therefore the variables $\zeta_1, \zeta_2, \dots, \zeta_n$ are mutually independent and of exponential distribution with the mean value 1. In this way, the random variables ξ_k^* themselves can be expressed in the form

$$\xi_k^* = F^{-1}(e^{-\zeta_{n+1-k}^*}) = F^{-1}\left(e^{-\left(\frac{\delta_1}{n} + \frac{\delta_2}{n-1} + \dots + \frac{\delta_{n+1-k}}{k}\right)}\right) \qquad (k = 1, 2, \dots, n); \tag{1.13}$$

where the variables $\delta_1, \delta_2, \dots, \delta_n$ are mutually independent and of exponential distribution with the same distribution function $1 - e^{-x}$ $(x > 0)$. It also follows from this result that the quotients

$$\frac{\eta_{k+1}^*}{\eta_k^*} = e^{-\frac{\delta_{n+1-k}}{k}} \tag{1.14}$$

are mutually independent random variables (here, by definition, $\eta_{n+1}^* \equiv 1$), since the variables δ_{n+1-k} are, as we have seen, mutually independent. Another consequence of (1.13) is that *the variables* $\xi_n^*, \xi_{n-1}^*, \dots, \xi_1^*$ *form a*

Markov chain (and thus the variables $\xi_1^*, \xi_2^*, \ldots, \xi_n^*$ form also a Markov chain); this follows from

(1. 15)
$$\xi_{n-k}^* = F^{-1}\left(e^{\log F(\xi_{n+1-k}^*) - \frac{\delta_{k+1}}{n-k}}\right)$$

which is obtained from (1.13) and from the fact that the variables ξ_{n+1-k}^* and δ_{k+1} are independent, since

$$\xi_{n+1-k}^* = F^{-1}\left(\exp\left[-\left(\frac{\delta_1}{n} + \frac{\delta_2}{n-1} + \cdots + \frac{\delta_k}{n-k+1}\right)\right]\right).$$

A. N. KOLMOGOROV [6a] was the first who remarked that the variables $\xi_1^*, \xi_2^*, \ldots, \xi_n^*$, i. e. the sequence of order statistics, form a Markov chain. The new method contained in the present paper starts from this fundamental observation, but the possibilities implied by it could be developed only after having transformed the Markov chain $\{\xi_k^*\}$ into an additive Markov chain by means of the transformation $\xi_k^* = \log \frac{1}{F(\xi_{n-k+1}^*)}$. In this connection it is interesting to consider the following general problem: for which Markov processes $\{\xi_t\}$ can such a family of functions $G_t(x)$ be found that the variables $\eta_t = G_t(\xi_t)$ form an additive Markov process? A necessary condition of this is that the distribution function $F(x, s, y, t) = \mathbf{P}(\xi_t < x \mid \xi_s = y)$ of the Markov process should satisfy the following differential equation:

$$\frac{\partial F}{\partial x}\frac{\partial F}{\partial y}\left(\frac{\partial F}{\partial y}\frac{\partial^3 F}{\partial x^2 \partial y} - \frac{\partial F}{\partial x}\frac{\partial^3 F}{\partial x \partial y^2}\right) = \frac{\partial^2 F}{\partial x \partial y}\left\{\frac{\partial^2 F}{\partial x^2}\left(\frac{\partial F}{\partial y}\right)^2 - \frac{\partial^2 F}{\partial y^2}\left(\frac{\partial F}{\partial x}\right)^2\right\}.$$

We hope to return to the discussion of this problem on another occasion.

The variables η_k are obviously uniformly distributed in the interval (0, 1), because, if $0 < x < 1$, then

(1. 16)
$$\mathbf{P}(\eta_k < x) = \mathbf{P}(\xi_k < F^{-1}(x)) = F(F^{-1}(x)) = x,$$

and therefore the variables η_k^* form an ordered sample of size n drawn from a population of uniform distribution in the interval (0, 1).

It follows from (1. 14) that

$$\left(\frac{\eta_{k+1}^*}{\eta_k^*}\right)^k = e^{-\delta_{n+1-k}}$$

and as $\mathbf{P}(e^{-\delta_{n+1-k}} < x) = \mathbf{P}\left(\delta_{n+1-k} > \log\frac{1}{x}\right) = e^{-\log\frac{1}{x}} = x$, therefore the variables $\left(\frac{\eta_{k+1}^*}{\eta_k^*}\right)^k$ are mutually independent and have the same distribution, namely, they are uniformly distributed in the interval (0, 1). This is the theorem of S. MALMQUIST mentioned in the introduction.

§ 2. The theory of order statistics built up by means of the method of § 1

On the basis of what has been said above it is easy to obtain the results concerning the limiting distribution of order statistics. In order to show this, we shall prove the following theorems.[4]

THEOREM 1. *If $k \geqq 1$ is a fixed positive integer, then*

$$\lim_{n\to\infty} \mathbf{P}(n\zeta_k^* < x) = \int_0^x \frac{t^{k-1}e^{-t}}{(k-1)!}\,dt \qquad (x>0),$$

i. e. $n\zeta_k^*$ has in the limit a Γ-distribution of order k.

PROOF. As we have seen,

$$\zeta_k^* = \frac{\delta_1}{n} + \frac{\delta_2}{n-1} + \cdots + \frac{\delta_k}{n+1-k}$$

where $\delta_1, \delta_2, \ldots, \delta_k$ are mutually independent and exponentially distributed random variables with the common distribution function $1-e^{-x}$ $(x>0)$. Therefore, the variable $\frac{\delta_j}{n+1-j}$ has the probability density function $(n+1-j)e^{-(n+1-j)x}$ $(x>0)$ and thus it follows by simple calculation that the probability density function of ζ_k^* is

$$g_k(t) = \binom{n}{k} k e^{-nt}(e^t-1)^{k-1};$$

hence $n\zeta_k^*$ has the frequency function

$$\text{(2. 1)} \qquad \frac{1}{n} g_k\left(\frac{t}{n}\right) = \binom{n-1}{k-1} e^{-t}(e^{\frac{t}{n}}-1)^{k-1} = \frac{[n(e^{\frac{t}{n}}-1)]^{k-1}e^{-t}\prod_{j=1}^{k-1}\left(1-\frac{j}{n}\right)}{(k-1)!}.$$

As $\lim_{n\to\infty} n(e^{\frac{t}{n}}-1) = t$, thus the density function of $n\zeta_k^*$ converges to $\frac{t^{k-1}e^{-t}}{(k-1)!}$ as $n\to\infty$, i. e. to the density function of the Γ-distribution of order k.

This result might have been expected by the following consideration. Obviously

$$\text{(2. 2)} \qquad n\zeta_k^* = \delta_1+\delta_2+\cdots+\delta_k+\sum_{j=2}^{k}\frac{(j-1)\delta_j}{n+1-j};$$

the density function of $\delta_1+\delta_2+\cdots+\delta_k$ is, however, $\frac{t^{k-1}e^{-t}}{(k-1)!}$, on the other hand, the variable $\sum_{j=2}^{k}\frac{(j-1)\delta_j}{n+1-j}$ tends stochastically to 0, as $n\to\infty$.

[4] We use the notations introduced in § 1.

To develop this consideration into a precise proof, we need the following lemma, due to H. CRAMÉR ([25], p. 254).

LEMMA 1. *Let us put $\gamma_n = \alpha_n + \beta_n$ where α_n and β_n are random variables and let $F_n(x)$ denote the distribution function of α_n and further let us assume that*[5]

$$\lim_{n\to\infty} \mathbf{M}\beta_n = 0 \quad \text{and} \quad \lim_{n\to\infty} \mathbf{D}\beta_n = 0.$$

Furthermore, let us suppose that there exists the limit $F(x)$ of the distribution functions $F_n(x)$ as $n \to \infty$, i. e.

$$\lim_{n\to\infty} F_n(x) = F(x)$$

holds for all points x of continuity of the distribution function $F(x)$. Further, let us denote the distribution function of γ_n by $G_n(x)$. Then

$$\lim_{n\to\infty} G_n(x) = F(x).$$

PROOF.[6] Without loss of generality we may suppose that $\mathbf{M}\beta_n = 0$. Then, by virtue of Tchebyshev's inequality, we have

$$\mathbf{P}(|\beta_n| > \varepsilon) < \frac{\mathbf{D}^2\beta_n}{\varepsilon^2},$$

therefore, given any, arbitrarily small $\varepsilon > 0$ and $\delta > 0$, there exists a positive integer $n_0(\delta)$ such that

$$\mathbf{P}(|\beta_n| > \varepsilon) < \delta \quad \text{if} \quad n > n_0(\delta).$$

But then

$$G_n(x) = \mathbf{P}(\gamma_n < x) \leqq \mathbf{P}(\alpha_n < x + \varepsilon) + \mathbf{P}(\beta_n < -\varepsilon). \tag{2.3}$$

In fact, if $\alpha_n + \beta_n < x$, then either $\alpha_n < x + \varepsilon$ or $\alpha_n \geqq x + \varepsilon$, but in the latter case at the same time $\beta_n < -\varepsilon$ holds and we obtain (2. 3) by means of the theorem on total probability. Similarly,

$$G_n(x) = \mathbf{P}(\gamma_n < x) \geqq \mathbf{P}(\alpha_n < x - \varepsilon) - \mathbf{P}(\beta_n > \varepsilon); \tag{2.4}$$

in fact, if $\alpha_n < x - \varepsilon$, then either $\alpha_n + \beta_n < x$, or $\alpha_n + \beta_n \geqq x$, but in the latter case at the same time $\beta_n > \varepsilon$. Consequently, we have

$$F_n(x - \varepsilon) - \delta \leqq G_n(x) \leqq F_n(x + \varepsilon) + \delta.$$

Passing to the limit $n \to \infty$ and considering that ε and δ can be chosen arbitrarily small, it follows that

$$F(x-0) \leqq \varliminf_{n\to\infty} G_n(x) \leqq \varlimsup_{n\to\infty} G_n(x) \leqq F(x+0),$$

[5] Here and in what follows we shall denote then mean value of the random variable ξ by $\mathbf{M}\xi$ and its standard deviation by $\mathbf{D}\xi$.

[6] We give here the proof of this lemma of CRAMÉR because a similar method of proof is needed in the proof of Lemma 2.

i. e., that in all points of continuity of $F(x)$

$$\lim_{n\to\infty} G_n(x) = F(x).$$

This proves Lemma 1.

Theorem 1 follows immediately from this lemma, as

$$\mathbf{M}\left(\sum_{j=2}^{k}\frac{(j-1)\delta_j}{n+1-j}\right)=\sum_{j=2}^{k}\frac{j-1}{n+1-j} \quad \text{and} \quad \mathbf{D}^2\left(\sum_{j=2}^{k}\frac{(j-1)\delta_j}{n+1-j}\right)=\sum_{j=2}^{k}\frac{(j-1)^2}{(n+1-j)^2}$$

and thus the conditions of Lemma 1 are satisfied.

By means of Theorem 1 we can easily determine also the limiting distribution of η_k^*. We have $\eta_{n+1-k}^* = e^{-\zeta_k^*}$ and therefore

$$\mathbf{P}(n(1-\eta_{n+1-k}^*) < x) = \mathbf{P}\left(\zeta_k^* < \log\frac{1}{1-\frac{x}{n}}\right);$$

since

$$\lim_{n\to\infty}\frac{\log\frac{1}{1-\frac{x}{n}}}{\frac{x}{n}} = 1$$

and the Γ-distribution is continuous, it follows that $n(1-\eta_{n+1-k}^*)$ has in limit also a Γ-distribution of order k with the density function $\frac{t^{k-1}e^{-t}}{(k-1)!}$ $(t>0)$. Now, the random variables η_k are mutually independent and uniformly distributed in the interval (0, 1). Because of the symmetry of the uniform distribution, the same holds also for the variables $1-\eta_k (k=1, 2, \ldots, n)$ and thus the variables

$$\eta_k^* = R_k(\eta_1, \eta_2, \ldots, \eta_n) \quad \text{and} \quad 1-\eta_{n+1-k}^* = R_k(1-\eta_1, 1-\eta_2, \ldots, 1-\eta_n)$$

have the same distribution. Hence it follows the following

THEOREM 2. *The distribution of the variables $n\eta_k^*$ and $n(1-\eta_{n+1-k}^*)$ in case of any fixed $k \geqq 1$, tends to the Γ-distribution of order k with the density function* $\frac{t^{k-1}e^{-t}}{(k-1)!}$ $(t>0)$.[7]

By means of Theorem 2 we can determine also the limiting distributions of ξ_k^* and ξ_{n+1-k}^*; these, however, — contrary to the limiting distributions of the variables η_k^* and ζ_k^* — will depend on the distribution function $F(x)$ (see [8]).

[7] The distribution of the variables η_k^* can be also determined exactly for finite n and after this passing to the limit Theorem 2 can be proved also in this manner by means of some simple calculations (see H. CRAMÉR [25]). We proved this theorem here by means of our method to show its application at first in a simple case.

Now we shall prove the following

THEOREM 3.[8] *The variables η_k^* and η_{n+1-j}^* are independent in the limit if $n\to\infty$ and at the same time k and j are fixed, namely*

$$\lim_{n\to\infty} \mathbf{P}\left(\eta_n^* < \frac{x}{n}, 1-\eta_{n+1-j}^* < \frac{y}{n}\right) = \int_0^x\int_0^y \frac{u^{k-1}v^{j-1}e^{-(u+v)}}{(k-1)!\,(j-1)!}\,du\,dv \qquad (x>0, y>0).$$

PROOF. First of all we prove a lemma:

LEMMA 2. *Let us put $\gamma_n = \alpha_n + \beta_n$ where α_n and β_n are random variables, and let a random variable χ_n be given which is independent of α_n. Let us denote the distribution functions of α_n and χ_n by $F_n(x)$ and $H_n(x)$ respectively. Let us assume that the limit functions $F(x) = \lim_{n\to\infty} F_n(x)$ and $H(x) = \lim_{n\to\infty} H_n(x)$ exist and, further, that*

$$\lim_{n\to\infty} \mathbf{M}\beta_n = 0 \quad \textit{and} \quad \lim_{n\to\infty} \mathbf{D}\beta_n = 0.$$

In case all these conditions are satisfied, we have

$$\lim_{n\to\infty} \mathbf{P}(\gamma_n < x; \chi_n < y) = F(x)\,H(y),$$

i. e., the variables γ_n and χ_n become independent in the limit.

PROOF. Let us choose (as in the proof of Lemma 1) the value of the integer n_0 so large that

$$\mathbf{P}(|\beta_n| > \varepsilon) < \delta \text{ if } n > n_0$$

Similarly to the arguments applied in the proof of Lemma 1, it may be proved that, if $n > n_0$, where n_0 depends on the choice of the positive numbers ε and δ, then

$$\text{(2.5)}\quad \mathbf{P}(\alpha_n < x-\varepsilon, \chi_n < y) - \delta \leqq \mathbf{P}(\gamma_n < x, \chi_n < y) \leqq \mathbf{P}(\alpha_n < x+\varepsilon, \chi_n < y) + \delta,$$

and as, by our assumption, α_n and χ_n are independent, therefore

$$\mathbf{P}(\alpha_n < x \pm \varepsilon, \chi_n < y) = F_n(x\pm\varepsilon)\,H_n(y)$$

and similarly to the proof of Lemma 1, we obtain that in all points of continuity of $F(x)$

$$\lim_{n\to\infty} \mathbf{P}(\gamma_n < x, \chi_n < y) = F(x)\,H(y)$$

holds. This completes the proof of Lemma 2.

Now

$$\zeta_{n+1-k}^* - \log n = \frac{\delta_{j+1}}{n-j} + \cdots + \frac{\delta_{n+1-k}}{k} - \log n + \zeta_j^*$$

[8] See CRAMÉR [25], p. 371. We discuss this well-known theorem here, because our method throws more light on the real ground of the fact expressed in the theorem, than its known proof.

where

$$\zeta_j^* = \frac{\delta_1}{n} + \frac{\delta_2}{n-1} + \cdots + \frac{\delta_j}{n+1-j},$$

and therefore

$$\lim_{n\to\infty} \mathbf{M}\zeta_j^* = \lim_{n\to\infty} \mathbf{D}\zeta_j^* = 0.$$

As the sum $\dfrac{\delta_{j+1}}{n-j} + \cdots + \dfrac{\delta_{n+1-k}}{k} - \log n$ is independent of ζ_j^* and

$$\lim_{n\to\infty} n \log \frac{1}{1-\dfrac{y}{n}} = y,$$

further, we know that

$$\lim_{n\to\infty} \mathbf{P}(n\zeta_j^* < y) = \int_0^y \frac{t^{j-1}}{(j-1)!} e^{-t}\, dt,$$

we have

$$\lim_{n\to\infty} \mathbf{P}\left(\eta_k^* < \frac{x}{n}, 1-\eta_{n+1-j}^* < \frac{y}{n}\right) = \lim_{n\to\infty} \mathbf{P}\left(\zeta_{n+1-k}^* - \zeta_j^* \geqq \log\frac{n}{x}\right) = \Gamma_j(y) \tag{2.6}$$

where

$$\Gamma_j(y) = \int_0^y \frac{t^{j-1}}{(j-1)!} e^{-t}\, dt,$$

On the other hand, by Lemma 1

$$\lim_{n\to\infty} \mathbf{P}\left(\zeta_{n+1-k}^* - \zeta_j^* \geqq \log\frac{n}{x}\right) = \lim_{n\to\infty} \mathbf{P}\left(\zeta_{n+1-k}^* \geqq \log\frac{n}{x}\right) \tag{2.7}$$

and by virtue of Theorem 2

$$\lim_{n\to\infty} \mathbf{P}\left(\zeta_{n+1-k}^* \geqq \log\frac{n}{x}\right) = \lim_{n\to\infty} \mathbf{P}\left(\eta_k^* < \frac{x}{n}\right) = \int_0^x \frac{t^{k-1}e^{-t}}{(k-1)!}\, dt. \tag{2.8}$$

From the relations (2.6), (2.7) and (2.8), Theorem 3 follows.

By means of Theorem 3 we can determine the limiting distribution of the difference $\eta_n^* - \eta_1^*$. This is important, because $\eta_n^* - \eta_1^*$, the range of the sample $(\eta_1, \eta_2, \ldots, \eta_n)$, can be used to estimate the standard deviation of the population. As, for large n, the variable η_n^* is near to 1 and η_1^* is near to 0 with a probability near to 1, we obviously have to consider the variable $n[1-(\eta_n^* - \eta_1^*)]$ and as, by virtue of Theorem 3, $n\eta_1^*$ and $n(1-\eta_n^*)$ are independent in the limit, the limiting distribution of their sum equals the composition of their limiting distributions. As e^{-x} $(x>0)$ is the density function of the limiting distribution of both $n\eta_1^*$ and $n(1-\eta_n^*)$, the density

function of the limiting distribution of $n[1-(\eta^*_n-\eta^*_1)]$ is

$$\int_0^x e^{-(x-y)}e^{-y}\,dy = xe^{-x} \qquad (x>0);$$

therefore $n[1-(\eta^*_n-\eta^*_1)]$ is in the limit a random variable having a Γ-distribution of order 2.

By means of the limiting distributions of the random variables η^*_k, the limiting distributions of the random variables ξ^*_k can also be determined.

Hitherto we have considered the limiting distributions of the order statistics ξ^*_k (resp. those of their transformed values η^*_k and ζ^*_k) under the condition that the index k (resp. $j=n+1-k$) is fixed and at the same time $n\to\infty$; this set of problems is called the study of the "extreme values" of the sample. We now turn to the study of the limiting distributions of the variables ξ^*_k (resp. of η^*_k and ζ^*_k) under the condition that together with n k tends also to infinity, namely so that $|k-nq| = o(\sqrt{n})$, where q is a constant $(0<q<1)$. The variable ξ^*_{k+1} (where $k=[nq]$)[9] satisfies this condition; this variable is called the *q-quantile* of the sample. In the special case $n=2m+1$ where m is an integer, the variable ξ^*_{m+1} is the median of the sample: obviously, the q-quantile of the sample is nothing else but the q-quantile of the sample distribution function and thus the median of the sample is nothing else but the median of the sample distribution function. Consequently, if n is an even integer, i. e. $n=2m$, then $\frac{1}{2}(\xi^*_m+\xi^*_{m+1})$ is called the median of the sample.

We shall now prove the following theorem containing the proposition that the q-quantiles of the sample in the limit are normally distributed, if the distribution function $F(x)$ of the population satisfies certain simple conditions.

THEOREM 4.[10] *Let us suppose that the density function $f(x)=F'(x)$ of the common distribution function $F(x)$ of the mutually independent random variables $\xi_1, \xi_2, \ldots, \xi_n$ exists and that $f(x)$ is continuous and positive in the interval $a<x<b$; then, if $0<F(a)<q<F(b)<1$ and further, if $|k_n-nq| = o(\sqrt{n})$ (and thus, a fortiori, $\lim\limits_{n\to\infty}\frac{k_n}{n}=q$), then $\xi^*_{k_n}$ is, in the limit, normally distributed with the mean value $Q=F^{-1}(q)$, which is the q-quantile of the distribution function $F(x)$, i. e.*

$$\lim_{n\to\infty}\mathbf{P}\left(\frac{\xi^*_{k_n}-Q}{\dfrac{1}{f(Q)}\sqrt{\dfrac{q(1-q)}{n}}}<x\right)=\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{x}e^{-\frac{t^2}{2}}\,dt.$$

[9] $[x]$ is the largest integer for which $[x]\leq x$.

[10] This theorem is contained in a general theorem of N. V. SMIRNOV [8g].

PROOF. First consider the limiting distribution of

$$\zeta^*_{n+1-k_n} = \sum_{j=1}^{n+1-k_n} \frac{\vartheta_j}{n+1-j} \tag{2.9}$$

where the variables ϑ_j are mutually independent and exponentially distributed with the distribution function $1-e^{-x}$ $(x>0)$, that is to say, $\mathbf{M}\vartheta_j = \mathbf{D}\vartheta_j = 1$ and

$$\mathbf{M}(|\vartheta_j - 1|^3) = \int_0^\infty |x-1|^3 e^{-x}\,dx < \int_0^1 e^{-x}\,dx + \int_0^\infty x^3 e^{-x}\,dx \leq 5.$$

Then, however,

$$\left\{\begin{aligned} M_n &= \mathbf{M}\zeta^*_{n+1-k_n} = \sum_{j=1}^{n+1-k_n} \frac{1}{n+1-j}, \\ S_n^2 &= \mathbf{D}^2\zeta^*_{n+1-k_n} = \sum_{j=1}^{n+1-k_n} \frac{1}{(n+1-j)^2}, \\ K_n^3 &= \sum_{j=1}^{n+1-k_n} \mathbf{M}\left|\frac{\vartheta_j - 1}{n+1-j}\right|^3 \leq 5 \sum_{j=1}^{n+1-k_n} \frac{1}{(n+1-j)^3}, \end{aligned}\right. \tag{2.10}$$

and thus

$$\frac{K_n}{S_n} \leq \frac{5}{k_n}. \tag{2.11}$$

Therefore, if $n\to\infty$, then $\frac{K_n}{S_n}\to 0$; this means that the central limit theorem in LIAPUNOV's form can be applied to the sequence of sums (2.9) and thus

$$\lim_{n\to\infty} \mathbf{P}\left(\frac{\zeta^*_{n+1-k_n} - M_n}{S_n} < x\right) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{-\frac{t^2}{2}}\,dt. \tag{2.12}$$

Now, it is known that

$$\sum_{k=1}^{m} \frac{1}{k} = \log m + C + \Delta_m$$

where C is the Euler constant, and an $A>0$ constant can be found such that $|\Delta_m| < \frac{A}{m}$. By means of some simple calculations it can be verified that

$$\sum_{k=h}^{H} \frac{1}{k^2} = \frac{1}{h} - \frac{1}{H} + \frac{\vartheta}{h(h-1)} \qquad (0<\vartheta<1). \tag{2.13}$$

Thus we have

$$M_n = \log\frac{n}{k_n} + \varepsilon_n', \tag{2.14}$$

$$S_n = \frac{1}{k_n} - \frac{1}{h} + \varepsilon_n'', \tag{2.15}$$

where $|\varepsilon_n'| < \frac{A}{k_n}$ and $|\varepsilon_n''| < \frac{B}{k_n^2}$, A and B being constants not depending on n. Therefore

$$\frac{\zeta^*_{n+1-k_n} - M_n}{S_n} = \frac{\zeta^*_{n+1-k_n} - \log \frac{n}{k_n}}{\sqrt{\frac{n-k_n}{n k_n}}} + \varepsilon_n''' \tag{2.16}$$

where $|\varepsilon_n'''| < L \sqrt{\frac{n}{k_n(n-k_n)}}$ and L is a constant not depending on n. But, if $n \to \infty$, then $\frac{k_n}{n} \to q$ and thus $\varepsilon_n''' \to 0$. Hence

$$\lim_{n \to \infty} \mathbf{P}\left(\frac{\zeta^*_{n+1-k_n} - \log \frac{n}{k_n}}{\sqrt{\frac{n-k_n}{n k_n}}} < x \right) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{-\frac{t^2}{2}} dt. \tag{2.17}$$

For brevity, let us introduce the notation $q_n = \frac{k_n}{n}$, then, by virtue of (2.17) and taking into account that owing to $|k_n - nq| = o(\sqrt{n})$, we have

$$\log \frac{1}{qn} - \log \frac{1}{q} = o\left(\frac{1}{\sqrt{n}}\right),$$

it follows that

$$\lim_{n \to \infty} \mathbf{P}\left(\frac{\zeta^*_{n+1-k_n} - \log \frac{1}{q}}{\sqrt{\frac{1-q}{nq}}} < x \right) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{-\frac{t^2}{2}} dt. \tag{2.18}$$

As $\zeta^*_{n+1-k_n} = \log \frac{1}{F(\xi^*_{k_n})}$, if follows from (2.18) that

$$\lim_{n \to \infty} \mathbf{P}\left(\xi^*_{k_n} > F^{-1}\left(q e^{-x\sqrt{\frac{1-q}{nq}}} \right) \right) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{-\frac{t^2}{2}} dt. \tag{2.19}$$

But, in view of the mean value theorem of differential calculus, we have

$$F^{-1}\left(q e^{-x\sqrt{\frac{1-q}{nq}}} \right) = Q + \frac{q\left(e^{-x\sqrt{\frac{1-q}{nq}}} - 1\right)}{f(Q\vartheta_n)} \tag{2.20}$$

where $\lim_{n \to \infty} \vartheta_n = 1$.

It follows that

$$\lim_{n \to \infty} \mathbf{P}\left(\frac{\xi^*_{k_n} - Q}{\frac{1}{f(Q)} \sqrt{\frac{q(1-q)}{n}}} < x \right) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{-\frac{t^2}{2}} dt, \tag{2.21}$$

which was to be proved.

The statement of our theorem can also be characterized by that the q-quantile of a sample of size n in case of large n is approximately normally distributed around Q, i. e. around the q-quantile of the population, with the standard deviation $\frac{1}{f(Q)}\sqrt{\frac{q(1-q)}{n}}$.

In this way, by means of the sample median, an interval containing the median of the population with probability arbitrarily near to 1, can be given. In the special case of symmetrical, for example, normal distribution, the median of the distribution coincides with its mean and in this way we can estimate the mean value of the population.

The theory of order statistics has a widespread applicability in the statistical quality control of mass production,[11] which is an important field of application of probability theory. Let us assume that a certain measurement of some engine parts produced on an automatic machine displays some small random fluctuations from specimen to specimen, therefore its value can be considered as a random variable. Let us suppose that, under standard manufacturing circumstances, the distribution function of this measurement is the (continuous) function $F(x)$; to control the process of production, at regular time intervals we draw a sample of size n — e. g. of size 5.

We take the considered measurement of the values of the sample and we mark them on a perpendicular straight line drawn across the abscissa corresponding to the point of time of sampling on the „control chart" and we mark their places with dots; the values of the sample will be placed automatically in order of magnitude. In order to detect any irregularity in the process of production (e. g. the displacement of the adjustment of the automatic machine or the attrition of certain parts of the producing machine etc.), we draw 5 bands determined by parallel straight lines, giving intervals containing the least, the second, the third, the fourth, and the largest value, respectively, of the sample of size 5 at the same time with a given probability — e. g. 95% — under standard manufacturing circumstances. The determination of these intervals is very easy by what has been said above. In fact, if ξ_k^* denotes the k-th sample value in order of magnitude ($k=1,2,3,4,5$), then, as we have seen, we can exactly determine the individual and joint distributions of the variables

$$\zeta_k^* = \log\frac{1}{F(\xi_{6-k}^*)} \qquad (k=1,2,3,4,5).$$

The practical application of this method in quality control is dealt with by the Department of Mathematical Statistics of the Institute for Applied

11 Cf. the work of L. I. Braginsky [26]; by means of the theory of order statistics, the calculations of Braginsky which are not quite exact can be put in a precise form; in the practical application it is suitable to carry out the control charts on the basis of these precise calculations.

Mathematics of the Hungarian Academy of Sciences; tables needed for the use of the method are also prepared.

We shall not continue the enumeration of theorems obtainable by means of this method, we only emphasize, that our method consists in deducing all these theorems, by means of (1. 9), from the theory of limiting distribution of sums of mutually independent random variables.

§ 3. Formulation of some new theorems concerning the comparison of the distribution function of a population and that of a sample drawn from it

Hitherto we have only shown how our method makes it possible to prove certain well-known results of order statistics. Now we shall show the new results which can be obtained by means of the same method.

A. N. KOLMOGOROV [6b] proved a fundamental theorem giving a test for the hypothesis that a sample has been drawn from a population having a given distribution. By means of this test we can infer to the unknown distribution of the population from the distribution of sample values.[12] Let us define

$$F_n(x)=\begin{cases} 0 & \text{if } x\leqq \xi_1^*, \\ \dfrac{k}{n} & \text{if } \xi_k^*<x\leqq \xi_{k+1}^*, \\ 1 & \text{if } \xi_n^*<x, \end{cases} \tag{3.1}$$

i. e. $F_n(x)$ is the distribution function of the sample, in other words, the frequency ratio of the values less than x in the sample.

KOLMOGOROV's theorem is as follows:

$$\lim_{n\to\infty} \mathbf{P}\left(\sqrt{n}\sup_{-\infty<x<+\infty}|F_n(x)-F(x)|<y\right)=\begin{cases} \sum\limits_{k=-\infty}^{\infty}(-1)^k e^{-2k^2y^2} & \text{if } y>0 \\ 0 & \text{if } y\leqq 0. \end{cases} \tag{3.2}$$

KOLMOGOROV's theorem therefore gives the limiting distribution of the supremum of absolute value of the difference between the distribution function of the sample and that of the population. This limiting distribution does not depend on the distribution function $F(x)$ of the population which is assumed, for the validity of theorem, to be continuous. KOLMOGOROV's theorem considers the difference $|F_n(x)-F(x)|$ with the same weight, regardless to the value of $F(x)$; so e. g. the difference $|F_n(x)-F(x)|=0{\cdot}01$ has the same weight in a point x with $F(x)=0{\cdot}5$ (where this difference is 2% of the value of $F(x)$) as a point x with $F(x)=0{\cdot}01$ (where this difference is 100%! of the value of $F(x)$). We can avoid this by considering the quotient $\dfrac{|F_n(x)-F(x)|}{F(x)}$ instead of $|F_n(x)-F(x)|$, that is to say, by considering the

[12] I. e. we can give confidence limits for the unknown distribution function.

relative error of $F_n(x)$. In this way, the idea arises, naturally, to consider the limiting distribution of the supremum of the quotient $\frac{|F_n(x)-F(x)|}{F(x)}$ which characterizes the relative deviation of distribution function of the population and that of the sample.

A theorem similar to that of KOLMOGOROV's was proved by N. V. SMIRNOV concerning the one-sided deviation of the sample and population distribution functions. SMIRNOV's theorem is as follows:

$$\lim_{n\to\infty} \mathbf{P}\left(\sqrt{n} \sup_{-\infty<x<+\infty} (F_n(x)-F(x)) < y\right) = \begin{cases} 1-e^{-2y^2} & \text{if } y>0, \\ 0 & \text{if } y \leqq 0. \end{cases} \tag{3.3}$$

We shall consider also the analogous problem for relative deviations.

All these problems can be successfully solved by means of the above method. In the course of solving these problems a natural limitation is to be adopted: as $F(x)$ takes on arbitrarily small values, it is not suitable to consider the supremum of $\frac{F_n(x)-F(x)}{F(x)}$ or respectively $\left|\frac{F_n(x)-F(x)}{F(x)}\right|$ taken in the whole interval $-\infty<x<+\infty$, but to restrict ourselves to an interval $x_a \leqq x < +\infty$, where the abscissa x_a is defined by the relation $F(x_a)=a>0$; the value of a, however, can be an arbitrarily small positive value. In § 5 we shall prove the following results:

THEOREM 5.

$$\lim_{n\to\infty} \mathbf{P}\left(\sqrt{n} \sup_{a\leqq F(x)} \frac{F_n(x)-F(x)}{F(x)} < y\right) = \begin{cases} \sqrt{\frac{2}{\pi}} \int\limits_0^{y\sqrt{\frac{a}{1-a}}} e^{-\frac{t^2}{2}}\, dt & \text{if } y>0, \\ 0 \quad \text{if } y \leqq 0. \end{cases} \tag{3.4}$$

THEOREM 6.

$$\lim_{n\to\infty} \mathbf{P}\left(\sqrt{n} \sup_{a\leqq F(x)} \left|\frac{F_n(x)-F(x)}{F(x)}\right| < y\right) = \begin{cases} \frac{4}{\pi} \sum\limits_{k=0}^{\infty} (-1)^k \frac{e^{-\frac{(2k+1)^2\pi^2}{8}\frac{1-a}{a y^2}}}{2k+1} & \text{if } y>0, \\ 0 \quad \text{if } y \leqq 0. \end{cases} \tag{3.5}$$

We may consider the limiting distribution of the supremum of $\frac{F_n(x)-F(x)}{F(x)}$, and of its absolute value taken in the interval $x_a \leqq x \leqq x_b$, respectively, where the abscissae x_a and x_b are defined by the relations $F(x_a)=a>0$ and $F(x_b)=b<1$ $(0<a<b<1)$. We then arrive at the following theorems.

THEOREM 7.

$$\lim_{n\to\infty} \mathbf{P}\left(\sqrt{n} \sup_{a\leq F(x)\leq b} \frac{F_n(x)-F(x)}{F(x)} < y\right) = \tag{3.6}$$

$$= \frac{1}{\pi} \int_{-\infty}^{y\sqrt{\frac{b}{1-b}}} e^{-\frac{u^2}{2}} \left(\int_0^{\left(\sqrt{\frac{b}{1-b}}y-u\right)\cdot\sqrt{\frac{a(1-b)}{b-a}}} e^{-\frac{t^2}{2}} dt \right) du \qquad (-\infty < y < +\infty).$$

THEOREM 8.

$$\lim_{n\to\infty} \mathbf{P}\left(\sqrt{n} \sup_{a\leq F(x)\leq b} \left| \frac{F_n(x)-F(x)}{F(x)} \right| < y\right) =$$

$$= \begin{cases} \dfrac{4}{\pi} \displaystyle\sum_{k=0}^{\infty} (-1)^k \frac{e^{-\frac{(2k+1)^2 \pi^2 (1-a)}{8 a y^2}}}{2k+1} E_k & \text{if } y > 0, \\ 0 \quad \text{if } y \leq 0; \end{cases} \tag{3.7}$$

where

$$E_k = 1 - \frac{2}{\sqrt{2\pi}} \int_{y\sqrt{\frac{b}{1-b}}}^{\infty} e^{-\frac{u^2}{2}} du + \varrho_k$$

and

$$\varrho_k = \frac{2e^{-\frac{b y^2}{2(1-b)}}}{\sqrt{2\pi}\sqrt{\frac{a}{1-a}}\, y} \int_0^{(2k+1)\frac{\pi}{2}} e^{\frac{(1-b)u^2}{2by^2}} \sin u\, du.$$

These theorems provide tests for verifying the hypothesis that the sample $(\xi_1, \xi_2, \ldots, \xi_n)$ has been drawn from a population of the distribution function $F(x)$. The character of these tests consists in that they give a band around $F(x)$ in which, if the hypothesis is true, the sample distribution function $F_n(x)$ have to lie with a certain probability and the width of this band in all points x being proportional to $F(x)$ This band, however, is not a symmetrical one. To overcome this difficulty, we apply the test twice, first to the sample $(\xi_1, \xi_2, \ldots, \xi_n)$ having the population distribution function $F(x)$ and then to the sample $(-\xi_1, -\xi_2, \ldots, -\xi_n)$ having the population distribution function $G(x) = 1 - F(-x)$. In order to illustrate this, let us denote the distribution function of the sàmple $(-\xi_1, -\xi_2, \ldots, -\xi_n)$ by $G_n(x)$ and let A be the event that

$$\sqrt{n} \sup_{a\leq F(x)} \left| \frac{F_n(x)-F(x)}{F(x)} \right| < y,$$

and B the event that

$$\sqrt{n} \sup_{a\leq F(x)} \left| \frac{G_n(x)-G(x)}{G(x)} \right| < y, \quad \text{i. e.,} \quad \sqrt{n} \sup_{F(x')\leq 1-a} \left| \frac{F_n(x')-F(x')}{1-F(x')} \right| < y;$$

finally, let us denote the simultaneous occurrence of A and B by C. Taking into account that

$$\mathbf{P}(C)=\mathbf{P}(AB)=\mathbf{P}(A)+\mathbf{P}(B)-\mathbf{P}(A+B)$$

and in case of occurrence $A+B$ we have obviously at the same time

$$\sqrt{n}\sup_{0\leqq F(x)\leqq 1}|F_n(x)-F(x)|<y;$$

and this last event, by KOLMOGOROV's theorem, has in the limit the probability

$$K(y)=\sum_{k=-\infty}^{\infty}(-1)^k e^{-2k^2y^2}, \tag{3.8}$$

Therefore $\mathbf{P}(A+B)\leqq K(y)$ in the limit and in the same case

$$\mathbf{P}(C)\geqq\mathbf{P}(A)+\mathbf{P}(B)-K(y).$$

The probabilities $\mathbf{P}(A)$ and $\mathbf{P}(B)$ are equal and their common value is given by (3.5). Thus the probability of the event that the sample distribution function $F_n(x)$ lies in the intersection of bands defined by the above two conditions corresponding to the sample $(\xi_1,\xi_2,\ldots,\xi_n)$ and $(-\xi_1,-\xi_2,\ldots,-\xi_n)$, respectively, is not less than $2L\left(y\sqrt{\frac{a}{1-a}}\right)-K(y)$ in the limit, where $L(z)=\sum_{k=0}^{\infty}(-1)^k\frac{e^{-\frac{(2k+1)^2\pi^2}{8z^2}}}{2(k+1)}$ $(z>0)$ and $K(y)$ is the function defined by (3.8).

Let us point out a most surprising corollary of Theorem 7. From the theorem (3.3) of SMIRNOV, we get

$$\lim_{n\to\infty}\mathbf{P}(\sup_{-\infty<x<+\infty}(F_n(x)-F(x))<0)=0, \tag{3.9}$$

i. e. the probability of the event that the sample distribution function does not exceed the population distribution function all along the interval $-\infty<x<+\infty$, tends to 0 as $n\to\infty$. From Theorem 5 it follows that

$$\lim_{n\to\infty}\mathbf{P}(\sup_{x_a\leqq x<+\infty}(F_n(x)-F(x))<0)=0, \tag{3.10}$$

i. e. the same is true for the interval $x_a\leqq x<+\infty$. On the other hand, by Theorem 7,

$$\lim_{n\to\infty}\mathbf{P}(\sup_{x_a\leqq x\leqq x_b}(F_n(x)-F(x))<0)=\frac{1}{\pi}\int_0^{\infty}e^{-\frac{u^2}{2}}\int_0^{u\sqrt{\frac{a(1-b)}{b-a}}}e^{-\frac{t^2}{2}}dt\,du>0, \tag{3.11a}$$

i. e. the probability of the event that the sample distribution function does not exceed the population distribution function all along the interval in which the value of $F(x)$ lies between arbitrarily fixed values a and b $(0<a<b<1)$, remains positive also in the limit. This result, obviously, is important also from the point of view of statistical practice.

The result that the limit on the left side of (3. 11a) is positive, was also proved by GIHMAN [16]; moreover, he obtained that

$$(3.\,11\text{b})\qquad \lim_{n\to\infty} \mathbf{P}\Big(\sup_{x_a\le x\le x_b}(F_n(x)-F(x))<0\Big)=\frac{1}{\pi}\arc\sin\sqrt{\frac{a(1-b)}{b(1-a)}}\,.$$

GIHMAN mentioned further that the result (3. 11b) has been already known to GNEDENKO. The terms on the right sides of (3. 11a) and (3. 11b) are, of course, identical. This follows from the following consideration: the right side of (3. 11a) is nothing else than two times the probability of the event that a random point normally distributed in the plane (x, y) and having the probability density function $\frac{1}{2\pi}e^{-\frac{1}{2}(x^2+y^2)}$, lies in the infinite sector $0<x<+\infty$, $0<y<x\sqrt{\frac{a(1-b)}{b-a}}$, and this probability is equal to

$$(3.\,12)\qquad \frac{2\arc\operatorname{tg}\sqrt{\frac{a(1-b)}{b-a}}}{2\pi}=\frac{1}{\pi}\arc\sin\sqrt{\frac{a(1-b)}{b(1-a)}}\,.$$

Indeed, because of the circular symmetry of the normal distribution having the density function $\frac{1}{2\pi}e^{-\frac{1}{2}(x^2+y^2)}$, the probability corresponding to the infinite sector of angle φ is $\frac{\varphi}{2\pi}$.

Theorems 5—8 will be proved in § 5. First in § 4 we shall prove some auxiliary theorems which are of interest in themselves too.

§ 4. Some new limiting distribution theorems

Let a sequence be given consisting of the sets of random variables

$$\xi_{n,1},\ \xi_{n,2},\ \ldots,\ \xi_{n,N_n}\qquad (n=1, 2, \ldots).$$

Let us assume that the random variables $\xi_{n,k}$ have the expectation 0 and a finite variance, further, that the random variables having the same first index n $(n=1, 2, \ldots)$ are mutually independent and satisfy LINDEBERG's condition, that is to say, introducing the notations

$$F_{n,k}(x)=\mathbf{P}(\xi_{n,k}<x);\quad S_{n,k}=\sum_{\nu=1}^{k}\xi_{n,\nu};\quad B_n^2=\mathbf{D}^2S_{n,N_n}=\sum_{k=1}^{N_n}\mathbf{D}^2\xi_{n,k},$$

we suppose

$$\mathbf{M}\xi_{n,k}=\int_{-\infty}^{\infty}x\,dF_{n,k}(x)=0,$$

and

$$(4.\,1)\qquad \lim_{n\to\infty}\frac{1}{B_n^2}\sum_{k=1}^{N_n}\int_{|x|>\varepsilon B_n}x^2dF_{n,k}(x)=0\quad\text{if}\quad \varepsilon>0.$$

Concerning these sequences satisfying the above conditions we shall prove the following theorems.

THEOREM 9.

$$\lim_{n\to\infty} \mathbf{P}(\max_{1\leqq k\leqq N_n} S_{n,k} < xB_n) = \begin{cases} \sqrt{\frac{2}{\pi}} \int_0^x e^{-\frac{t^2}{2}}\,dt & \text{if } x>0, \\ 0 \quad \text{if} \quad x \leqq 0. \end{cases} \tag{4.2}$$

THEOREM 10.

$$\lim_{n\to\infty} \mathbf{P}(\max_{1\leqq k\leqq N_n} |S_{n,k}| < xB_n) = \begin{cases} \frac{4}{\pi} \sum_{k=0}^{\infty} (-1)^k \frac{e^{-\frac{(2k+1)^2\pi^2}{8x^2}}}{2k+1} & \text{if } x>0, \\ 0 \quad \text{if} \quad x \leqq 0 \end{cases} \tag{4.3}$$

THEOREM 11.

$$\lim_{n\to\infty} \mathbf{P}(-yB_n \leqq \min_{1\leqq k\leqq N_n} S_{n,k} \leqq \max_{1\leqq k\leqq N_n} S_{n,k} < xB_n) = \tag{4.4}$$

$$= \begin{cases} \frac{4}{\pi} \sum_{k=0}^{\infty} \frac{e^{-\frac{(2k+1)^2\pi^2}{2(x+y)^2}} \sin (2k+1)\pi \frac{x}{x+y}}{2k+1} & \text{if } x>0 \text{ and } y \geqq 0, \\ 0 \quad \text{if either} \quad x\leqq 0 \quad \text{or} \quad y<0. \end{cases}$$

REMARK. In case $y=x$, Theorem 11 reduces to Theorem 10.

THEOREM 12. *Let* $A_n^2 = \mathbf{D}^2 S_{n, M_n}$ *with* $1 \leqq M_n < N_n$ *and*

$$\lim_{n\to\infty} \frac{A_n}{B_n} = \lambda \qquad (0 \leqq \lambda < 1).$$

Then

$$\lim_{n\to\infty} \mathbf{P}(\max_{M_n<k\leqq N_n} |S_{n,k}| < yB_n) = \tag{4.5}$$

$$= \begin{cases} \frac{4}{\pi} \sum_{k=0}^{\infty} (-1)^k \frac{e^{-\frac{(2k+1)^2\pi^2}{8y^2}}}{2k+1} \left(1 - \frac{2}{\sqrt{2\pi}} \int_{\frac{y}{\lambda}}^{\infty} e^{-\frac{u^2}{2}}\,du + \varrho_k\right) & \text{if } y>0, \\ 0 \quad \text{if} \quad y\leqq 0 \end{cases}$$

where

$$\varrho_k = \frac{2\lambda e^{-\frac{y^2}{2\lambda^2}}}{\sqrt{2\pi}y} \int_0^{(2k+1)\frac{\pi}{2}} e^{\frac{\lambda^2u^2}{2y^2}} \sin u\,du.$$

REMARK. In the special case of $M_n=1$ (i. e. for $\lambda=0$), Theorem 12 is identical with Theorem 10.

For the special case in which all the considered random variables $\xi_{n,k}$ have the same distribution, Theorems 9 and 10 were proved by P. ERDŐS

and M. KAC [22].[12] In the proofs of the above more general theorems, we modify their proofs inasmuch as we apply an ordinary (one-dimensional) limiting distribution theorem instead of the multi-dimensional limit theorem used by them; this enables us to generalize their results. We shall use Theorems 9—12 in § 5 to determine the limiting distribution of the random variables

$$\sup_{a \leqq F(x) \leqq b} \frac{F_n(x) - F(x)}{F(x)} \quad \text{and} \quad \sup_{a \leqq F(x) \leqq b} \left| \frac{F_n(x) - F(x)}{F(x)} \right|$$

where $F_n(x)$ denotes again the distribution function of a sample of n mutually independent observations concerning the random variable ξ having a continuous distribution function $F(x)$ and further $0 < a < b \leqq 1$.

Let us turn to the proof of Theorem 9. Let us put

$$P_n(x) = \mathbf{P}(\max_{1 \leqq k \leqq N_n} S_{n,k} < x B_n).$$

Let $\eta_1, \eta_2, \ldots, \eta_n, \ldots$ be mutually independent random variables which are normally distributed with mean 0 and variance 1, and let us introduce the random variables

$$\zeta_k = \sum_{\nu=1}^{k} \eta_\nu \qquad (k = 1, 2, \ldots).$$

First of all we shall prove that for any $\varepsilon > 0$ and for any positive integer k we have

$$\underline{\lim}_{n \to \infty} P_n(x) \geqq \mathbf{P}(\max(\zeta_1, \zeta_2, \ldots, \zeta_k) < (x - \varepsilon)\sqrt{k}) - \frac{1}{\varepsilon^2 k} \tag{4.6}$$

and

$$\overline{\lim}_{n \to \infty} P_n(x) \leqq \mathbf{P}(\max(\zeta_1, \zeta_2, \ldots, \zeta_k) < x\sqrt{k}). \tag{4.7}$$

For, let m_j be the least positive integer satisfying

$$\sum_{r=1}^{m_j} \mathbf{D}^2 \xi_{n,r} \geqq \frac{j}{k} B_n^2$$

$(j = 1, 2, \ldots, k)$. Obviously, $1 \leqq m_1 \leqq m_2 \leqq \ldots \leqq m_k = N_n$. Let us define now the following variables:

$$\Delta_{n,1} = S_{n,m_1}; \quad \Delta_{n,j} = S_{n,m_j} - S_{n,m_{j-1}} \qquad (j = 2, 3, \ldots, k). \tag{4.8}$$

We can see easily that for any fixed j $(j = 1, 2, \ldots, k)$ the Lindeberg condition holds for the sequence

$$\xi_{n,m_{j-1}+1}, \xi_{n,m_{j-1}+2}, \ldots, \xi_{n,m_j} \qquad (n = 1, 2, 3, \ldots). \tag{4.9}$$

[12] Their method was generalized by M. D. DONSKER [20b]. See further the papers by A. WALD [27], [28], and K. L. CHUNG [29]. They consider the limiting distributions of the supremum of the first n partial sums under the conditions that the variables have the same distribution and that the variables have finite third moments, respectively. CHUNG gives for this latter special case an estimate for the remainder term also. ERDŐS and KAC remarked that their theorems can be proved under more general conditions.

Indeed, introducing the notation

$$B_{n,j}^2 = \mathbf{D}^2 \Delta_{n,j}$$

and using the relation

$$\lim_{n\to\infty} \frac{1}{B_n^2} \sup_{1\leq k\leq N_n} \mathbf{D}^2 \xi_{n,k} = 0$$

which trivially follows from (4. 1), we obtain that, for any $\delta > 0$,

$$\frac{1-\delta}{k} B_n^2 \leqq B_{n,j}^2 \leqq \frac{1+\delta}{k} B_n^2, \quad \text{if} \quad n > n_0(\delta) \tag{4. 10}$$

holds. Thus for any $\varepsilon > 0$

$$\frac{1}{B_{n,j}^2} \sum_{r=m_{j-1}+1}^{m_j} \int_{|x|>\varepsilon B_{n,j}} x^2\, dF_{n,r}(x) \leqq \frac{k}{1-\delta} \frac{1}{B_n^2} \sum_{r=1}^{N_n} \int_{|x|>\varepsilon' B_n} x^2\, dF_{n,r}(x)$$

if $n > n_0(\delta)$, and $\varepsilon' = \varepsilon \sqrt{\frac{1-\delta}{k}}$. The Lindeberg condition is therefore actually satisfied by the sequence (4. 9). Therefore, by the central limit theorem,

$$\lim_{n\to\infty} \mathbf{P}(\Delta_{n,j} < x B_{n,j}) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{-\frac{t^2}{2}} dt \qquad (j = 1, 2, \ldots, k). \tag{4. 11}$$

But the random variables $\Delta_{n,1}, \Delta_{n,2}, \ldots, \Delta_{n,k}$ are mutually independent and

$$\lim_{n\to\infty} \frac{B_{n,j}}{B_n} = \frac{1}{\sqrt{k}} \qquad (j = 1, 2, \ldots, k);$$

hence

$$\lim_{n\to\infty} \mathbf{P}\left(\frac{\Delta_{n,j}}{B_n} < \frac{x_j}{\sqrt{k}};\ j = 1, 2, \ldots, k\right) = \tag{4. 12}$$

$$= \frac{1}{(\sqrt{2\pi})^k} \int_{-\infty}^{x_1} \int_{-\infty}^{x_2} \cdots \int_{-\infty}^{x_k} e^{-\frac{1}{2}\left(\sum_{j=1}^{k} t_j^2\right)} dt_1 \ldots dt_k$$

i. e.

$$\lim_{n\to\infty} \mathbf{P}\left(\frac{\Delta_{n,1} + \Delta_{n,2} + \cdots + \Delta_{n,j}}{B_n} < x;\ j = 1, 2, \ldots, k\right) = \tag{4. 13}$$

$$= \frac{1}{(\sqrt{2\pi})^k} \iint_{(T_x)} \cdots \int e^{-\frac{1}{2}\left(\sum_{j=1}^{k} t_j^2\right)} dt_1\, dt_2 \ldots dt_k;$$

where the integration is to be extended over the domain T_x defined by

$$T_x:\ \{-\infty < t_1 + t_2 + \cdots + t_j < x\sqrt{k};\ j = 1, 2, \ldots, k\}.$$

Hence we obtain

$$\lim_{n\to\infty} \mathbf{P}(\max_{1\leq j\leq k} S_{n,m_j} < x B_n) = \mathbf{P}(\max_{1\leq j\leq k} \zeta_j < x\sqrt{k}). \tag{4. 14}$$

Let us put

$$Q_{n,k}(x) = \mathbf{P}(\max_{1 \leq j \leq k} S_{n,m_j} < xB_n),$$

and let $\Pi_{n,r}(x)$ denote the probability of the event that $S_{n,r}$ is the first of the sums $S_{n,j}$ $(j=1,2,\ldots,r)$ which is $\geqq xB_n$, i. e. let

$$\Pi_{n,r}(x) = \mathbf{P}(S_{n,r} \geqq xB_n;\ \max_{1 \leq j \leq r-1} S_{n,j} < xB_n).$$

Obviously,

$$\sum_{r=1}^{N_n} \Pi_{n,r}(x) = 1 - P_n(x) \leqq 1.$$

Let us suppose $m_{j-1} < r \leqq m_j$; introducing the notations

$$\Pi_{n,r}^{(1)}(x) = \mathbf{P}(S_{n,r} \geqq xB_n;\ \max_{1 \leq j \leq r-1} S_{n,j} < xB_n;\ |S_{n,m_j} - S_{n,r}| \geqq \varepsilon B_n)$$

and

$$\Pi_{n,r}^{(2)}(x) = \mathbf{P}(S_{n,r} \geqq xB_n;\ \max_{1 \leq j \leq r-1} S_{n,j} < xB_n;\ |S_{n,m_j} - S_{n,r}| < \varepsilon B_n).$$

we get evidently

$$\Pi_{n,r}(x) = \Pi_{n,r}^{(1)}(x) + \Pi_{n,r}^{(2)}(x).$$

Let us apply TCHEBYSHEV's inequality:

$$\Pi_{n,r}^{(1)}(x) = \Pi_{n,r}(x)\mathbf{P}(|S_{n,m_j} - S_{n,r}| \geqq \varepsilon B_n) \leqq \Pi_{n,r}(x)\frac{B_{n,j}^2}{\varepsilon^2 B_n^2}$$

and consider the relation (4. 10); thus we obtain that

$$\Pi_{n,r}^{(1)}(x) \leqq \Pi_{n,r}(x)\frac{1+\delta}{\varepsilon^2 k};$$

therefore

$$1 - P_n(x) = \sum_{r=1}^{N_n} \Pi_{n,r}(x) \leqq \frac{1+\delta}{\varepsilon^2 k} + \sum_{r=1}^{N_n} \Pi_{n,r}^{(2)}(x). \tag{4. 15}$$

On the other hand,

$$\sum_{r=1}^{N_n} \Pi_{n,r}^{(2)}(x) \leqq 1 - Q_{n,k}(x-\varepsilon) \tag{4. 16}$$

as from the relations

$$S_{n,r} \geqq xB_n \quad \text{and} \quad |S_{n,m_j} - S_{n,r}| < \varepsilon B_n$$

it follows that

$$S_{n,m_j} > (x-\varepsilon)B_n.$$

Thus we have

$$1 - P_n(x) \leqq \frac{1+\delta}{\varepsilon^2 k} + 1 - Q_{n,k}(x-\varepsilon).$$

Further, on account of the trivial inequalities $P_n(x) \leqq Q_{n,k}(x)$ $(k=1,2,\ldots)$, we obtain

$$Q_{n,k}(x-\varepsilon) - \frac{1+\delta}{\varepsilon^2 k} \leqq P_n(x) \leqq Q_{n,k}(x). \tag{4. 17}$$

Comparing the above relation (4.17) with (4.14), we have just the desired inequalities (4.6) and (4.7).

Let us consider now the special case in which the variables $\xi_{n,k}$ assume only the values $+1$ and -1, and

$$\mathbf{P}(\xi_{n,k}=+1)=\mathbf{P}(\xi_{n,k}=-1)=\frac{1}{2} \qquad (k=1,2,\ldots,N_n=n;\ n=1,2,\ldots).$$

Then

$$(4.18) \qquad \mathbf{P}_n(x)=\frac{1}{2^n}\sum_{\substack{-n<\nu<[x\sqrt{n}]\\ \nu\equiv n \bmod 2}}\left[\binom{n}{\frac{n+\nu}{2}}-\binom{n}{\frac{n-\nu}{2}+[x\sqrt{n}+1]}\right]$$

(except if $x\sqrt{n}$ is an integer) and thus from the Moivre—Laplace theorem we conclude that

$$(4.19) \qquad \lim_{n\to\infty} P_n(x)=\sqrt{\frac{2}{\pi}}\int_0^x e^{-\frac{t^2}{2}}dt \qquad (x>0).$$

Therefore, as it follows from (4.6) that

$$(4.20) \qquad \overline{\lim_{k\to\infty}}\,\mathbf{P}(\max(\zeta_1,\zeta_2,\ldots,\zeta_k)<x\sqrt{k})\leqq\underline{\lim_{n\to\infty}}\,P_n(x+\varepsilon)$$

and from (4.7) that

$$(4.21) \qquad \underline{\lim_{k\to\infty}}\,\mathbf{P}(\max(\zeta_1,\zeta_2,\ldots,\zeta_k)<x\sqrt{k})\geqq\overline{\lim_{n\to\infty}}\,P_n(x),$$

we have

$$(4.22) \qquad \lim_{k\to\infty}\mathbf{P}(\max(\zeta_1,\zeta_2,\ldots,\zeta_k)<x\sqrt{k})=\sqrt{\frac{2}{\pi}}\int_0^x e^{-\frac{t^2}{2}}dt \qquad (x>0),$$

and, applying again the relations (4.6) and (4.7), we obtain (4.2).

The basic idea of this proof can be summed up as follows: we have pointed out that in case of a special choice of the variables $\xi_{n,k}$, (4.2) holds; from this, by (4.6) and (4.7), we have concluded that (4.2) is true also in case $\xi_{n,k}=\eta_n$ where the variables η_n are normally distributed; hence, again by (4.6) and (4.7), it followed that (4.2) holds also for any variables $\xi_{n,k}$ satisfying the conditions of the theorem.

The proof of Theorems 10 and 11 is based on the same idea and, with suitable modifications, agrees step by step with the proof of Theorem 9.

It is sufficient to prove only Theorem 11, because this, as we have seen, includes Theorem 10 as a special case. It is unnecessary to detail the first part of the proof, therefore we shall deal only with the second.

Let us have again

$$\mathbf{P}(\xi_{n,k}=+1)=\mathbf{P}(\xi_{n,k}=-1)=\frac{1}{2} \qquad (k=1,2,\ldots,N_n=n;\ n=1,2\ldots)$$

and let us suppose that the variables $\xi_{n,k}$ $(k=1,2,\ldots,N_n=n)$ are mutually

independent. Then it follows by simple arguments, well-known in the theory of the random walk in the plane, that, if $A=[x\sqrt{n}]+1$ and $B=[y\sqrt{n}]+1$, then

(4. 23) $$\mathbf{P}(-y\sqrt{n}<S_{n,k}<x\sqrt{n};\ k=1,2,\ldots,n)=$$
$$=\sum_{-B<k<A}\left\{v_k+\sum_{\nu=1}^{\infty}(v_{2\nu(A+B)+k}-v_{2\nu(A+B)-2B-k}+v_{-2\nu(A+B)+k}-v_{-2\nu(A+B)+2A-k})\right\}$$

where
$$v_k=\begin{cases}\binom{n}{\frac{n+k}{2}}\frac{1}{2^n} & \text{if}\quad k\equiv n\ (\text{mod}\ 2)\\ 0 & \text{in all other cases.}\end{cases}$$

As, by the Moivre—Laplace theorem,
$$\lim_{n\to\infty}\left(\sum_{\frac{n}{2}-b\frac{\sqrt{n}}{2}<k<\frac{n}{2}+a\frac{\sqrt{n}}{2}}\binom{n}{k}\frac{1}{2^n}\right)=\frac{1}{\sqrt{2\pi}}\int_{-b}^{a}e^{-\frac{t^2}{2}}dt,$$

by simple calculation we obtain

(4. 24) $$\lim_{n\to\infty}\mathbf{P}(-y\sqrt{n}<S_{n,k}<x\sqrt{n};\ k=1,2,\ldots,n)=$$
$$=\frac{4}{\pi}\sum_{k=0}^{\infty}\frac{e^{-\frac{(2k+1)^2\pi^2}{2(x+y)^2}}\sin(2k+1)\pi\frac{x}{x+y}}{2k+1}\qquad(x>0,\ y>0).$$

Similarly to the case of Theorem 9, it follows that the limit of the probability on the left side of (4. 4) is the same also in the general case.

Theorem 12 can be derived from Theorem 11 as follows. Owing to the independence of S_{n,M_n} and $S_{n,k}-S_{n,M_n}$ $(k>M_n)$, by the relation
$$\mathbf{P}(\max_{M_n<k\leqq N_n}|S_{n,k}|<yB_n)=\mathbf{P}(-yB_n<(S_{n,M_n}+(S_{n,k}-S_{n,M_n}))<yB_n),$$

we obtain, by virtue of the theorem on total probability, that

(4. 25) $$\mathbf{P}(\max_{M_n<k\leqq N_n}|S_{n,k}|<yB_n)=$$
$$=\int_{-\infty}^{\infty}\mathbf{P}(-(x+y)B_n<S_{n,k}-S_{n,M_n}<(y-x)B_n)d\mathbf{P}\left(\frac{S_{n,M_n}}{B_n}<x\right).$$

As, in accordance with our restrictions, Lindeberg's condition is satisfied by the sums $S_{n,M_n}=\sum_{k=1}^{M_n}\xi_{n,k}$, further, $\mathbf{D}\left(\frac{S_{n,M_n}}{B_n}\right)=\frac{A_n}{B_n}\to\lambda$, as $n\to\infty$, therefore (uniformly in x in all finite intervals) we have

(4. 26) $$\lim_{n\to\infty}\mathbf{P}\left(\frac{S_{n,M_n}}{B_n}<x\right)=\frac{1}{\sqrt{2\pi}\lambda}\int_{-\infty}^{x}e^{-\frac{u^2}{2\lambda^2}}du=\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\frac{x}{\lambda}}e^{-\frac{t^2}{2}}dt.$$

Furthermore, by Theorem 11, considering the relation

$$\mathbf{D}(S_{n,N_n}-S_{n,M_n})=\sqrt{B_n^2-A_n^2},$$

it follows that

(4.27) $$\lim_{n\to\infty}\mathbf{P}(-(x+y)B_n<S_{n,k}-S_{n,M_n}<(y-x)B_n;\ k=1,2,\ldots,n)=$$

$$=\begin{cases}\dfrac{4}{\pi}\displaystyle\sum_{k=0}^{\infty}\frac{e^{-\frac{(2k+1)^2\pi^2(1-\lambda^2)}{8y^2}}}{2k+1}\sin(2k+1)\pi\frac{y-x}{2y}, & \text{if } y>0 \text{ and } |x|\leqq y,\\ 0 \text{ if } y\leqq 0 \text{ or } y>0 \text{ but } |x|>y.\end{cases}$$

Therefore, finally, we obtain

(4.28) $$\lim_{n\to\infty}\mathbf{P}(\max_{M_n<k\leqq N_n}|S_{n,k}|<yB_n)=$$

$$=\frac{4}{\pi}\sum_{k=0}^{\infty}\frac{e^{-\frac{(2k+1)^2\pi^2(1-\lambda^2)}{8y^2}}}{2k+1}\int_{-y}^{+y}\frac{e^{-\frac{x^2}{2\lambda^2}}}{\sqrt{2\pi}\lambda}\sin(2k+1)\pi\frac{y-x}{2y}\,dx.$$

Hence, by simple calculations, we obtain Theorem 12. In fact,

(4.29) $$\int_{-y}^{+y}\frac{e^{-\frac{x^2}{2\lambda^2}}}{\sqrt{2\pi}\lambda}\sin(2k+1)\pi\frac{y-x}{2y}\,dx=$$

$$=(-1)^k e^{-\frac{(2k+1)^2\pi^2\lambda^2}{8y^2}}\left(\int_{-\frac{y}{\lambda}}^{+\frac{y}{\lambda}}\frac{e^{-\frac{1}{2}\left(t-\frac{(2k+1)i\lambda}{2y}\pi\right)^2}}{\sqrt{2\pi}}\,dt\right).$$

Now, since the integral of $e^{-\frac{t^2}{2}}$ on any closed curve vanishes, therefore, if $a>0$ and b is real, then

$$\int_{-a}^{+a}\frac{e^{-\frac{(t-ib)^2}{2}}}{\sqrt{2\pi}}\,dt=\int_{-a-ib}^{a-ib}\frac{e^{-\frac{t^2}{2}}}{\sqrt{2\pi}}\,dt=\int_{-a}^{+a}\frac{e^{-\frac{t^2}{2}}}{\sqrt{2\pi}}\,dt+\int_{-a-ib}^{-a}\frac{e^{-\frac{t^2}{2}}}{\sqrt{2\pi}}\,dt+\int_{a}^{a-ib}\frac{e^{-\frac{t^2}{2}}}{\sqrt{2\pi}}\,dt=$$

$$=\int_{-a}^{a}\frac{e^{-\frac{t^2}{2}}}{\sqrt{2\pi}}\,dt+\frac{2e^{-\frac{a^2}{2}}}{\sqrt{2\pi}}\int_0^b e^{\frac{v^2}{2}}\sin av\,dv.$$

Consequently,

$$\int_{-y}^{+y}\frac{e^{-\frac{x^2}{2\lambda^2}}}{\sqrt{2\pi}\lambda}\sin(2k+1)\pi\frac{y-x}{2y}\,dy=$$

$$=(-1)^k e^{-\frac{(2k+1)^2\pi^2\lambda^2}{8y^2}}\left(1-\frac{2}{\sqrt{2\pi}}\int_{\frac{y}{\lambda}}^{\infty}e^{-\frac{t^2}{2}}\,dt+\frac{2e^{-\frac{y^2}{2\lambda^2}}\lambda}{\sqrt{2\pi}\,y}\int_0^{(2k+1)\frac{\pi}{2}}e^{\frac{\lambda^2v^2}{2y^2}}\sin v\,dv\right).$$

This completes the proof of Theorem 12.

§ 5. Proof of the tests analogous to those of Kolmogorov and Smirnov

Let ξ be a random variable having the continuous distribution function $F(x)$ and let $\xi_1, \xi_2, \ldots, \xi_n$ denote the results of n independent observations for the value of ξ, i. e. let $\xi_1, \xi_2, \ldots, \xi_n$ be mutually independent random variables having the same continuous distribution function $F(x)$. Let us denote the distribution function of this sample by $F_n(x)$.

We shall prove the theorems formulated in § 3 by means of the method exposed in § 1, using the theorems of § 4.

Let us put $\eta_k = F(\xi_k)$ and $\zeta_k = \log \frac{1}{\eta_k}$, further, $\eta_k^* = F(\xi_k^*)$ and $\zeta_k^* = R_k(\zeta_1, \zeta_2, \ldots, \zeta_n)$. In this case the variables η_k are uniformly distributed in the interval $(0, 1)$ and their sample distribution function is

$$G_n(x) = F_n(F^{-1}(x))$$

where $y = F^{-1}(x)$ is the inverse function of $x = F(y)$. But it is easily seen that

$$\sup_{a \leqq F(x)} \left(\frac{F_n(x) - F(x)}{F(x)} \right) = \sup_{a \leqq x \leqq 1} \frac{G_n(x) - x}{x}, \tag{5. 1}$$

therefore, instead of the variable on the left side of (5. 1), we may consider the variable $\sup\limits_{a \leqq x \leqq 1} \frac{G_n(x) - x}{x}$ identical with it. The variables η_k^* — as we have seen — form a Markov chain. Further, we have seen that the variables $\delta_{k+1} = (n-k)(\zeta_{k+1}^* - \zeta_k^*)$ are mutually independent and exponentially distributed with mean 1, i. e.

$$\mathbf{P}(\delta_k < x) = 1 - e^{-x} \qquad (x > 0).$$

We have also seen how the variables $\zeta_k^* = \log \frac{1}{\eta_{n+1-k}^*}$ may be decomposed into sums of mutually independent random variables by means of the δ_j's:

$$\zeta_k^* = \sum_{j=1}^{k} \frac{\delta_j}{n+1-j}.$$

Let us turn to the proof of Theorem 8. First of all, it is easy to see that instead of the relation (3. 4) it is enough to prove

$$\lim_{n \to \infty} \mathbf{P}\left(\sqrt{n} \sup_{a \leqq G_n(x)} \frac{G_n(x) - x}{x} < y \right) = \sqrt{\frac{2}{\pi}} \int_0^{y\sqrt{\frac{a}{1-a}}} e^{-\frac{t^2}{2}} dt \qquad (y > 0). \tag{5. 2}$$

For, if $|G_n(x) - x| \leqq \varepsilon$, then from $G_n(x) \geqq a + \varepsilon$ it follows that $x \geqq G_n(x) - \varepsilon \geqq a$ and thus

$$\sup_{a \leqq x} \frac{G_n(x) - x}{x} \geqq \sup_{G_n(x) \geqq a+\varepsilon} \frac{G_n(x) - x}{x}$$

i. e. from $\sup\limits_{a \leqq x} \frac{G_n(x)-x}{x} < \frac{y}{\sqrt{n}}$ it follows that $\sup\limits_{G_n(x) \geqq a+\varepsilon} \frac{G_n(x)-x}{x} < \frac{y}{\sqrt{n}}$. But if A, A' and B are any events and $AB \subset A'B$, then

$$\mathbf{P}(A) = \mathbf{P}(A\bar{B}) + \mathbf{P}(AB) \leqq \mathbf{P}(\bar{B}) + \mathbf{P}(A'B) \leqq \mathbf{P}(\bar{B}) + \mathbf{P}(A').$$

Applying this inequality to the case when A is the event $\sup\limits_{a \leqq x} \frac{G_n(x)-x}{x} < \frac{y}{\sqrt{n}}$, B is the event $|G_n(x)-x| \leqq \varepsilon$, and, finally, A' denotes the event $\sup\limits_{G_n(x) \geqq a+\varepsilon} \frac{G_n(x)-x}{x} < \frac{y}{\sqrt{n}}$, we obtain

$$\mathbf{P}\left(\sqrt{n} \sup_{a \leqq x} \frac{G_n(x)-x}{x} < y\right) \leqq \mathbf{P}(|G_n(x)-x| > \varepsilon) + \mathbf{P}\left(\sqrt{n} \sup_{a+\varepsilon \leqq G_n(x)} \frac{G_n(x)-x}{x} < y\right).$$

It can be similarly shown that

$$\mathbf{P}\left(\sqrt{n} \sup_{a-\varepsilon \leqq G_n(x)} \frac{G_n(x)-x}{x} < y\right) \leqq \mathbf{P}(|G_n(x)-x| > \varepsilon) + \mathbf{P}\left(\sqrt{n} \sup_{a \leqq x} \frac{G_n(x)-x}{x} < y\right).$$

As

$$\lim_{n\to\infty} \mathbf{P}(|G_n(x)-x| > \varepsilon) = 0 \qquad (\varepsilon > 0),$$

it follows that if (5. 2) is satisfied then

$$\overline{\lim_{n\to\infty}}\, \mathbf{P}\left(\sqrt{n} \sup_{a \leqq x} \frac{G_n(x)-x}{x} < y\right) \leqq \sqrt{\frac{2}{\pi}} \int_0^{y\sqrt{\frac{a+\varepsilon}{1-a-\varepsilon}}} e^{-\frac{t^2}{2}}\, dt$$

and

$$\underline{\lim_{n\to\infty}}\, \mathbf{P}\left(\sqrt{n} \sup_{a \leqq x} \frac{G_n(x)-x}{x} < y\right) \geqq \sqrt{\frac{2}{\pi}} \int_0^{y\sqrt{\frac{a-\varepsilon}{1-a+\varepsilon}}} e^{-\frac{t^2}{2}}\, dt.$$

Since ε can be chosen arbitrarily small and the integral is a continuous function of its upper limit, it follows that

$$\lim_{n\to\infty} \mathbf{P}\left(\sqrt{n} \sup_{a \leqq x} \frac{G_n(x)-x}{x} < y\right) = \sqrt{\frac{2}{\pi}} \int_0^{y\sqrt{\frac{a}{1-a}}} e^{-\frac{t^2}{2}}\, dt.$$

Therefore, (3. 4) actually follows from (5. 2) and thus, to prove Theorem 8, it is enough to show that (5. 2) holds.

Further, we shall need the following relation:

$$\sqrt{n} \sup_{a \leqq G_n(x)} \frac{G_n(x)-x}{x} = \sqrt{n} \max_{an \leqq k \leqq n} \left(\frac{\frac{k}{n}}{\eta_k^*} - 1\right). \tag{5. 3}$$

This follows from the fact that $G_n(x)$ is a constant lying between η_k^* and

η^*_{k+1}, and so in any interval $\eta^*_k < x < \eta^*_{k+1}$ the supremum of $\frac{G_n(x)-x}{x} = \frac{G_n(x)}{x} - 1$ is equal to

$$\frac{G_n(\eta^*_k+0)}{\eta^*_k} - 1 = \frac{\frac{k}{n}}{\eta^*_k} - 1.$$

Now, let us apply Theorem 9 to the sequence consisting of the following sequence of random variables:

$$\frac{\delta_j - 1}{n+1-j} \qquad (j = 1, 2, \ldots, [n(1-a)]+1);$$

this sequence satisfies LINDEBERG's condition (and, moreover, even LIAPUNOV's condition) if $0 < a < 1$. Then, by (1. 11), for any $z > 0$, we obtain

$$(5.4)\quad \lim_{n\to\infty} \mathbf{P}\left(\max_{an\leq k\leq n}\left(\log\frac{1}{\eta^*_k} - \sum_{\nu=k}^{n}\frac{1}{\nu}\right) < z\sqrt{\sum_{an\leq k=n}\frac{1}{k^2}}\right) = \sqrt{\frac{2}{\pi}}\int_0^z e^{-\frac{t^2}{2}}\,dt.$$

As in case of $k \geqq an$ and $0 < a < 1$,

$$\sum_{\nu=k}^{n}\frac{1}{\nu} = \log\frac{n}{k} + O\left(\frac{1}{n}\right) \quad\text{and}\quad \sqrt{\sum_{an\leq k\leq n}\frac{1}{k^2}} = \sqrt{\frac{1-a}{an}} + O\left(\frac{1}{n}\right),$$

from (5. 4) one concludes

$$(5.5)\qquad \lim_{n\to\infty}\mathbf{P}\left(\max_{an\leq k\leq n}\log\frac{\frac{k}{n}}{\eta^*_k} < z\sqrt{\frac{1-a}{an}}\right) = \sqrt{\frac{2}{\pi}}\int_0^z e^{-\frac{t^2}{2}}\,dt;$$

therefore, finally, introducing the notation $y = z\sqrt{\frac{1-a}{a}}$, we have

$$(5.6)\qquad \lim_{n\to\infty}\mathbf{P}\left(\sqrt{n}\max_{an\leq k\leq n}\log\left(\frac{\frac{k}{n}}{\eta^*_k} - 1\right) < y\right) = \sqrt{\frac{2}{\pi}}\int_0^{y\sqrt{\frac{a}{1-a}}} e^{-\frac{t^2}{2}}\,dt.$$

In view of (5. 2) and (5. 3), Theorem 5 follows from (5. 6).

Let us now turn to the proof of Theorem 7. We may obtain the random variable

$$(5.7)\qquad \tau = \sqrt{n}\max_{an\leq k\leq bn}\left(\log\frac{1}{\eta^*_k} - \sum_{\nu=k}^{n}\frac{1}{\nu}\right) = \sqrt{n}\max_{an\leq k\leq bn}\sum_{j=1}^{n+1-k}\frac{\delta_j - 1}{n+1-j}$$

as the sum of to independent random variables τ_1 and τ_2 where

$$(5.8)\qquad \tau_1 = \sqrt{n}\sum_{1\leq j\leq n+1-bn}\frac{\delta_j-1}{n+1-j}$$

and

$$(5.9)\qquad \tau_2 = \sqrt{n}\max_{an\leq n+1-k\leq bn}\sum_{j=1}^{k}\frac{\delta_j-1}{n+1-j}.$$

It is evident that in the limit τ_1 is a normally distributed random variable with the standard deviation $\sqrt{\frac{1-b}{b}}$; further, from the proof of Theorem 5 we can see that

$$\lim_{n\to\infty} \mathbf{P}(\tau_2\sqrt{b} < z) = \sqrt{\frac{2}{\pi}} \int_0^{z\sqrt{\frac{a}{b-a}}} e^{-\frac{t^2}{2}}\,dt \qquad (z>0). \tag{5.10}$$

Considering further that τ_1 and τ_2 are independent, it follows from (5.8) and (5.10) that

$$\lim_{n\to\infty} \mathbf{P}(\tau < y) = \frac{1}{\pi}\sqrt{\frac{b}{1-b}} \int_{-\infty}^{y} e^{-\frac{bu^2}{2(1-b)}} \int_0^{(y-u)\sqrt{\frac{ab}{b-a}}} e^{-\frac{t^2}{2}}\,dt\,du. \tag{5.11}$$

This completes the proof of Theorem 7.

In the same way we can also prove Theorem 6. Here the relation (5.3) is replaced by

$$\sqrt{n} \sup_{a\leqq G_n(x)} \left|\frac{G_n(x)-x}{x}\right| = \sqrt{n} \max_{an\leqq k\leqq n} \left(\left|\frac{\frac{k}{n}}{\eta_k^*}-1\right|, \left|\frac{\frac{k}{n}}{\eta_{k-1}^*}-1\right|\right) \tag{5.12}$$

from which it follows

$$\begin{aligned}\sqrt{n} \max_{an\leqq k\leqq n} \left|\frac{\frac{k}{n}}{\eta_k^*}-1\right| &\leqq \sqrt{n} \sup_{a\leqq G_n(x)} \left|\frac{G_n(x)-x}{x}\right| \leqq \\ &\leqq \sqrt{n} \max_{an\leqq k\leqq n} \left|\frac{\frac{k}{n}}{\eta_k^*}-1\right| + \frac{1}{a\sqrt{n}}.\end{aligned} \tag{5.13}$$

For, if $\eta_{k+1}^* < \frac{k}{n}$, then $\left|\frac{\frac{k}{n}}{\eta_{k+1}^*}-1\right| = \frac{\frac{k}{n}}{\eta_{k+1}^*}-1 < \frac{\frac{k+1}{n}}{\eta_{k+1}^*}-1 = \left|\frac{\frac{k+1}{n}}{\eta_{k+1}^*}-1\right|$; if, however, $\eta_{k+1}^* \geqq \frac{k}{n}$, then in case $k\geqq an$, $\eta_{k+1}^* \geqq a$ and thus

$$\left|\frac{\frac{k}{n}}{\eta_{k+1}^*}-1\right| = 1-\frac{\frac{k}{n}}{\eta_{k+1}^*} \leqq 1-\frac{\frac{k+1}{n}}{\eta_{k+1}^*}+\frac{1}{n\eta_{k+1}^*} \leqq \left|\frac{\frac{k+1}{n}}{\eta_{k+1}^*}-1\right|+\frac{1}{an}.$$

Consequently, in either case

$$\left|\frac{\frac{k}{n}}{\eta_{k+1}^*}-1\right| \leqq \left|\frac{\frac{k+1}{n}}{\eta_{k+1}^*}-1\right|+\frac{1}{an} \qquad (k\geqq an)$$

and since $\max\limits_{an\leq k\leq n}\left|\dfrac{\frac{k+1}{n}}{\eta^*_{k+1}}-1\right|\leq\max\limits_{an\leq k\leq n}\left|\dfrac{\frac{k}{n}}{\eta^*_k}-1\right|$, we get

$$\max_{an\leq k\leq n}\left(\left|\frac{\frac{k}{n}}{\eta^*_k}-1\right|,\ \left|\frac{\frac{k}{n}}{\eta^*_{k+1}}-1\right|\right)\leq\max_{an\leq k\leq n}\left|\frac{\frac{k}{n}}{\eta^*_k}-1\right|+\frac{1}{an}.$$

The limiting distribution of the variable

$$\sqrt{n}\max_{an\leq k\leq n}\left|\frac{\frac{k}{n}}{\eta^*_k}-1\right|$$

occurring here is identical with that of the variable

$$\sqrt{n}\max_{an\leq k\leq n}\left|\log\frac{1}{\eta^*_k}\sum_{\nu=k}^{n}\frac{1}{\nu}\right|=\sqrt{n}\max_{an\leq k\leq n}\left|\sum_{j=1}^{n+1-k}\frac{\delta_j-1}{n+1-j}\right|,$$

which can be determined by means of Theorem 10.

To prove Theorem 8, those steps have to be applied simultaneously which have been used in the proof of Theorems 6 and 7; in this proof we shall use Theorem 12 instead of Theorem 10.

The basic idea of the proof is as follows. The limiting distribution of the variable

$$\sqrt{n}\sup_{a\leq F(x)\leq b}\left|\frac{F_n(x)-F(x)}{F(x)}\right|$$

is identical with that of the variable

$$\varkappa_1=\sqrt{n}\max_{an\leq k\leq bn}\left|\frac{\frac{k}{n}}{\eta^*_k}-1\right|,$$

and therefore it is identical also with that of the variable

$$\varkappa_2=\sqrt{n}\max_{an\leq k\leq bn}\left|\log\frac{\frac{k}{n}}{\eta^*_k}\right|=\sqrt{n}\max_{an\leq k\leq bn}\left|\sum_{j=1}^{n+1-k}\frac{\delta_j-1}{n+1-j}\right|.$$

Thus Theorem 12 is applicable, namely, since the values of the constants A_n and B_n occurring in it, are as follows:

$$A_n=\sqrt{\frac{1-b}{bn}}+o\left(\frac{1}{n}\right)\quad\text{and}\quad B_n=\sqrt{\frac{1-a}{an}}+o\left(\frac{1}{n}\right),$$

therefore

$$\lambda=\lim_{n\to\infty}\frac{A_n}{B_n}=\sqrt{\frac{a(1-b)}{b(1-a)}},$$

and thus introducing the notation $S_{n,r}=\sum_{j=1}^{r}\frac{\delta_j-1}{n+1-j}$, we have

$$\lim_{n\to\infty}\mathbf{P}\left(\sqrt{n}\sup_{a\leq F(x)\leq b}\left|\frac{F_n(x)-F(x)}{F(x)}\right|<y\right)=$$

$$=\lim_{n\to\infty}\mathbf{P}\left(\max_{n+1-bn\leq r\leq n+1-an}|S_{n,r}|<y\sqrt{\frac{a}{1-a}}B_n\right)=$$

$$=\frac{4}{\pi}\sum_{k=0}^{\infty}(-1)^k\frac{e^{-\frac{(2k+1)^2\pi^2}{8}\frac{1-a}{ay^2}}}{2k+1}\left(1-\frac{2}{\sqrt{2\pi}}\int_{y\sqrt{\frac{b}{1-b}}}^{\infty}e^{-\frac{u^2}{2}}du+\varrho_k\right)$$

where

$$\varrho_k=\frac{2\sqrt{\frac{1-b}{b}}e^{-\frac{by^2}{2(1-b)}}}{\sqrt{2\pi}\,y}\int_0^{(2k+1)\frac{\pi}{2}}e^{\frac{u^2(1-b)}{2by^2}}\sin u\,du.$$

This completes the proof of Theorem 8.

§. 6. Remarks on the limiting distribution functions occurring in Theorems 5—8

The values of the limiting distribution function occurring in Theorem 5 may be read from the tables of the normal distribution function. The values of the limiting distribution function occurring in Theorem 6 can be computed by substituting the values $z=y\sqrt{\frac{a}{1-a}}$ into the function

$$L(z)=\frac{4}{\pi}\sum_{k=0}^{\infty}(-1)^k\frac{\exp\left(-\frac{(2k+1)^2\pi^2}{8z^2}\right)}{2k+1}\qquad(z>0).\tag{6.1}$$

At the end of this paper, we give the table of the function $L\left(y\sqrt{\frac{a}{1-a}}\right)$ for certain values of a. The curve of the distribution function $L\left(y\sqrt{\frac{a}{1-a}}\right)$ can for certain values of a be seen on Fig. 1.

The values of the limiting distribution function occurring in Theorem 7 can be approximatively computed in the following manner:

$$F(y,a,b)=\frac{1}{\pi}\int_{-\infty}^{y\sqrt{\frac{b}{1-b}}}e^{-\frac{u^2}{2}}\int_0^{\left(y-u\sqrt{\frac{1-b}{b}}\right)\sqrt{\frac{ab}{b-a}}}e^{-\frac{v^2}{2}}dv\,du=\frac{1}{\pi}\iint_T e^{-\frac{u^2+v^2}{2}}du\,dv\tag{6.2}$$

where T is an infinite triangular domain in the plane (u, v) defined by the following inequalites:

$$(6.3) \quad T: \left\{ -\infty < u < y\sqrt{\frac{b}{1-b}};\ 0 \leqq v \leqq \sqrt{\frac{a(1-b)}{b-a}}\left(y\sqrt{\frac{b}{1-b}}-u\right) \right\}.$$

Introducing the polar coordinates $r=\sqrt{u^2+v^2}$, $\varphi = \operatorname{arc\,tg}\frac{v}{u}$ we obtain

$$(6.4) \qquad F(y, a, b) = \frac{1}{\pi}\int_0^{\pi-\alpha}\left(1-e^{-\frac{ay^2}{2(1-a)\sin^2(\varphi+\alpha)}}\right)d\varphi$$

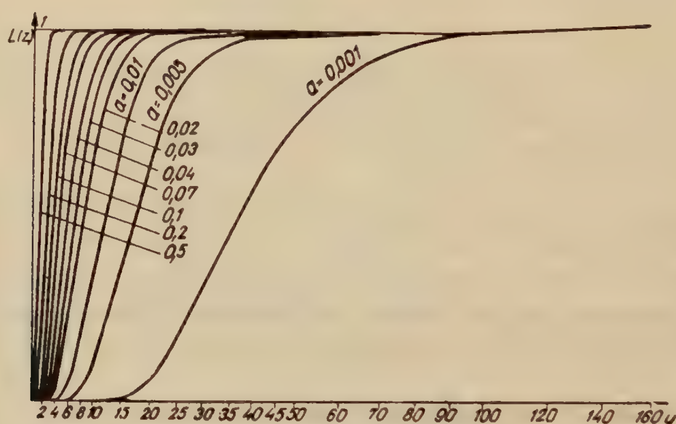


Fig. 1.

where $\operatorname{tg}\alpha = \sqrt{\frac{a(1-b)}{b-a}}$ and $0<\alpha<\frac{\pi}{2}$; therefore

$$(6.5) \qquad F(y, a, b) = \frac{1}{\pi}\int_\alpha^{\pi}\left(1-e^{-\frac{ay^2}{2(1-a)\sin^2\beta}}\right)d\beta.$$

As

$$(6.6) \qquad \frac{1}{\pi}\int_0^{\pi}\left[1-\exp\left(-\frac{a y^2}{2(1-a)\sin^2\beta}\right)\right]d\beta = \sqrt{\frac{2}{\pi}}\int_0^{y\sqrt{\frac{a}{1-a}}} e^{-\frac{u^2}{2}}\,du,$$

we have finally the following approximative expression:

$$(6.7) \qquad F(y, a, b) = \sqrt{\frac{2}{\pi}}\int_0^{y\sqrt{\frac{a}{1-a}}} e^{-\frac{u^2}{2}}\,du - \frac{\operatorname{arc\,tg}\sqrt{\frac{a(1-b)}{b-a}}}{\pi}(1-R)$$

where

$$(6.8)\quad R=\frac{1}{\alpha}\int_0^{\alpha}\exp\left(\frac{ay^2}{2(1-a)\sin^2\beta}\right)d\beta \quad\text{and}\quad \alpha=\operatorname{arc\,tg}\sqrt{\frac{a(1-b)}{b-a}}.$$

If $1-b=\varepsilon$ is small, then R is, in most cases, negligible, except for extremely small values of y, since

$$(6.9)\qquad R\leqq\exp\left(-\frac{ay^2}{2(1-a)\sin^2\alpha}\right)=\exp\left(-\frac{by^2}{2(1-b)}\right).$$

The values of the limiting distribution function occurring in Theorem 8 can be approximatively computed in the following manner: it follows from the second mean value theorem of the integral calculus that

$$(6.10)\qquad |\varrho_k|=\frac{2e^{-\frac{by^2}{2(1-b)}}\sqrt{\frac{1-b}{b}}}{\sqrt{2\pi}y}\left|\int_0^{(2k+1)\frac{\pi}{2}}e^{-\frac{(1-b)u^2}{2by^2}}\sin u\,du\right|\leqq$$

$$\leqq\frac{2e^{-\frac{by^2}{2(1-b)}}\sqrt{\frac{1-b}{b}}}{\sqrt{2\pi}y}\exp\left(\frac{(2k+1)^2\pi^2(1-b)}{8by^2}\right).$$

In this way, using the notation (6.1) the limiting distribution function occurring in Theorem 8 can be expressed in the following form

$$(6.11)\qquad \frac{4}{\pi}L\left(y\sqrt{\frac{a}{1-a}}\right)\left(1-\frac{2}{\sqrt{2\pi}}\int_{y\sqrt{\frac{b}{1-b}}}e^{-\frac{u^2}{2}}du\right)+\Delta$$

where, as is seen by way of a simple calculation.

$$(6.12)\qquad \Delta<\frac{2\lambda e^{-\frac{by^2}{2(1-b)}}}{\pi\sqrt{2\pi}y}\log\frac{1+\exp\left(-\frac{\pi^2(b-a)}{8aby^2}\right)}{1-\exp\left(-\frac{\pi^2(b-a)}{8aby^2}\right)},$$

whence it is readily seen that if b is very near to 1, Δ is negligible. Observe that the first factor of the main term depends only on a, the second only on b; this fact simplifies the computation to a great extent; namely, because we can obtain the first factor from the table of $L(z)$, the second from the table of the normal distribution function.

Institute for Applied Mathematics
of the Hungarian Academy of Sciences.

(Received 30 October 1953)

Bibliography

[1] K. Pearson, Note on Francis Galton's problem, *Biometrika*, **1** (1902), pp. 390—399.

[2] L. v. Bortkiewicz, Variationsbreite und mittlere Fehler, *Sitzungsber. Berl. Math. Ges.*, **21** (1922), pp. 3—11.

[3] E. L. Dodd, The greatest and the least variate under general laws of error, *Trans. Amer. Math. Soc.*, **25** (1923), pp. 525—539.

[4] L. H. C. Tippet, On the extreme individuals and the range of samples taken from a normal population, *Biometrika*, **17** (1925), pp. 264—387.

[5] M. Fréchet, Sur la loi de probabilité de l'écart maximum, *Ann. Soc. Polon. Math.*, **6** (1928), pp. 92—116.

[6] a) A. N. Kolmogorov, Sulla determinazione empirico di una legge di distribuzione, *Giornale dell'Istituto Italiano d. Attuari*, **4** (1933), pp. 83—91.

b) A. N. Kolmogorov, Confidence limits for an unknown distribution function, *Ann. Math. Stat.*, **12** (1941), pp. 461—463.

[7] V. I. Glivenko, Sulla determinazione empirica delle leggi di probabilità, *Giorn. Ist. Ital. Attuari*, **4** (1933), pp. 92—99.

[8] a) N. V. Smirnov, Über die Verteilung des allgemeinen Gliedes in der Variationsreihe, *Metron*, **12** (1935), pp. 59—81.

b) Н. В. Смирнов, Sur la distribution de ω^2, *Comptes Rendus Ac. Sci., Paris*, **202** (1936), pp. 449—452.

c) Н. В. Смирнов, О распределении ω^2-критерия Мизеса, Матем. Сборник, **2 (44)** (1937), pp. 973—994.

d) Н. В. Смирнов, Об уклонениях эмпирической кривой распределения, Матем. Сборник, **6 (44)** (1939), pp. 3—26.

e) Н. В. Смирнов, Оценка расхождения между эмпирическими кривыми распределения в двух независимых выборках, Бюлл. Моск. Унив., **2** (1939), pp. 3—14.

f) Н. В. Смирнов, Приближение законов распределения случайных величин по эмпирическим данным, Успехи Мат. Наук, **10** (1944), pp. 176—206.

g) Н. В. Смирнов, Предельные законы распределения для членов вариационного ряда, Труды Мат. Инст. Стеклова, **25** (1949), pp. 1—60.

[9] B. V. Gnedenko, Limit theorems for sums of independent random variables, *Transactions Amer. Math. Soc.*, **45** (1951), pp.

[10] Б. В. Гнеденко и В. С. Королюк, О максимальном расхождение двух эмпирических распределений, Докл. Акад. Наук СССР, **80** (1951), pp. 525—528.

[11] Б. В. Гнеденко и Е. Л. Рвачева, Об одной задаче сравнения двух эмпирических распределений, Докл. Акад. Наук СССР, **82** (1952), pp. 513—516.

[12] Б. В. Гнеденко и В. С. Михалевич, Две теоремы о поведений эмпирических функций распределения, Докл. Акад. Наук СССР, **82** (1952), pp. 841—843 and pp. 25—27.

[13] В. С. Михалевич, О взаимном расположений двух эмпирических функций распределения, Докл. Акад. Наук СССР, **85** (1952), pp. 485—488.

[14] И. Д. Квит, О теореме Н. В. Смирнова относительно сравнения двух выборок, Докл. Акад. Наук СССР, **71** (1950), pp. 229—231.

[15] Г. М. Мания, Обобщение критерия А. Н. Колмогорова для оценки закона распределения по эмпирическим данным, Докл. Акад. Наук СССР, **69** (1949), pp. 495—497.

[16] И. И. Гихман, Об эмпирической функций распределения в случае группировки данных, Докл. Акад. Наук СССР. **82** (1952), pp. 837—840.

[17] W. Feller, On the Kolmogorov—Smirnov limit theorems for empirical distributions, *Ann. Math. Statistics*, **19** (1948), pp. 177—180.

[18] J. L. Doob, Heuristic approach to the Kolmogorov—Smirnov theorems, *Ann. Math. Statistics*, **20** (1949), pp. 393—403.

[19] a) F. J. Massey, A note on the estimation of a distribution function by confidence limits, *Ann. Math. Statistics*, **21** (1950), pp. 116—119.

b) F. J. Massey, A note on the power of a non-parametric test, *Ann. Math. Statistics*, **21** (1950), pp. 440—443.

c) F. J. Massey, Distribution table for the deviation between two sample cumulatives, *Ann. Math. Statistics*, **23** (1952), pp. 435—441.

[20] a) M. D. Donsker, Justification and extension of Doob's heuristic approach to the Kolmogorov—Smirnov theorems, *Ann. Math. Statistics*, **23** (1952), pp. 277—281,

b) M. D. Donsker, An invariance principle for certain probability limit theorems, *Memoirs Amer. Math. Soc.*, **6** (1951), pp. 1—12.

[21] T. W. Anderson—D. A. Darling, Asymptotic theory of certain „goodness of fit" criteria based on stochastic processes, *Ann. Math. Statistics*, **23** (1952), pp. 193—212

[22] P. Erdős—M. Kac, On certain limit theorems of the theory of probability, *Bull. Amer Math. Soc.*, **52** (1946), pp. 292—302.

[23] S. Malmquist, On a property of order statistics from a rectangular distribution, *Skand. Aktuerietidsskrift*, **33** (1950), pp. 214—222.

[24] G. Hajós and A. Rényi, Elementary proofs of some basic facts concerning order statistics, *Acta Math. Acad. Sci. Hung.*, **5** (1954) (under press).

[25] H. Cramér, *Mathematical methods of statistics* (Princeton, 1946).

[26] Л. И. Брагински, Оперативный статистический контроль качества в машиностроении (Москва, 1951), Машгиз.

[27] A. Wald, Limit distribution of the maximum and minimum of successive cumulative sums of random variables, *Bull. Amer. Math. Soc.*, **53** (1947), pp. 142—153.

[28] A. Wald, On the distribution of the maximum of successive cumulative sums of independently, but not indentically distributed chance variables, *Bull. Amer. Math. Soc.*, **54** (1948), pp. 422—430.

[29] K. L. Chung, Asymptotic distribution of the maximum cumulative sum of independent random variables, *Bull. Amer. Math. Soc.*, **54** (1948), pp. 1162—1170.

[30] S. S. Wilks, Order statistics, *Bull. Amer. Math. Soc.*, **54** (1948), pp. 6—50.

y \ a	0,01	0,02	0,03	0,04	0,05	0,06	0,07	0,08	0,09	0,1	0,2	0,3	0,4	0,5
0,1													0,0000	0,0000
0,5											0,0000	0,0000	0,0008	0,0092
1,0						0,0000	0,0000	0,0000	0,0000	0,0000	0,0092	0,0716	0,2001	0,3708
1,5			0,0000	0,0000	0,0000	0,0002	0,0009	0,0023	0,0050	0,0092	0,1420	0,3543	0,5591	0,7328
2,0		0,0000	0,0001	0,0008	0,0036	0,0101	0,0212	0,0367	0,0563	0,0791	0,3708	0,6193	0,7951	0,9082
2,5		0,0001	0,0022	0,0112	0,0299	0,0578	0,0925	0,1320	0,1730	0,2155	0,5778	0,7966	0,9714	0,9751
3,0	0,0000	0,0015	0,0157	0,0474	0,0941	0,1487	0,2061	0,2632	0.3184	0,3708	0,7328	0,9009	0,9915	0,9954
3,5	0,0001	0,0092	0,0491	0,1135	0,1879	0,2629	0,3341	0,3994	0,4598	0,5140	0,8398	0,9561	0,9978	0,9991
4,0	0,0006	0,0291	0,1052	0,2001	0,2942	0,3804	0,4570	0,5244	0,5835	0,6353	0,9082	0,9823	0,9995	0,9999
4,5	0,0031	0,0643	0,1776	0,2950	0,4001	0,4902	0,5665	0,6311	0,6860	0,7328	0,9511	0,9936	0,9999	1,0000
5,0	0,0096	0,1135	0,2582	0,3895	0,4985	0,5873	0,6594	0,7193	0,7683	0,8088	0,9751	0,9979	1,0000	
5,5	0,0225	0,1726	0,3511	0,4784	0,5863	0,6723	0.7374	0,7903	0,8326	0,8665	0,9887	0,9994		
6,0	0,0428	0,2375	0,4204	0,5591	0,6627	0,7409	0,8006	0,8463	0,8817	0,9081	0,9954	0,9999		
6,5	0,0707	0,3045	0,4952	0,6310	0,7282	0,7989	0,8509	0,8895	0,9181	0,9395	0,9977	1,0000		
7,0	0,1053	0,3708	0,5639	0,6939	0,7834	0,8461	0,8904	0,9220	0,9446	0,9607	0,9991			
7,5	0,1452	0,4347	0,6193	0,7484	0,8294	0,8839	0,9207	0,9460	0,9633	0,9752	0,9996			
8,0	0,1889	0,4959	0,6811	0,7951	0,8671	0,9135	0,9436	0,9634	0,9763	0,9847	0,9999			
8,5	0,2348	0,5513	0,7301	0,8345	0,8977	0,9365	0,9606	0,9756	0,9850	0,9908	1,0000			
9,0	0,2819	0,6032	0,7731	0,8696	0,9221	0,9540	0,9729	0,9849	0,9907	0,9946				
9,5	0,3290	0,6510	0,8104	0,8950	0,9410	0,9713	0,9817	0,9898	0,9944	0,9969				
10,0	0,3754	0,6938	0,8427	0,9175	0,9564	0,9770	0,9878	0,9936	0,9967	0,9983				
10,5	0,4205	0,7328	0,8704	0,9358	0,9680	0,9840	0,9921	0,9961	0,9981	0,9991				
11,0	0,4640	0,7678	0,8939	0,9505	0,9768	0,9891	0,9949	0,9976	0,9989	0,9995				
11,5	0,5055	0,7992	0,9137	0,9622	0,9833	0,9927	0,9968	0,9986	0,9994	0,9997				
12,0	0,5450	0,8271	0,9303	0,9713	0,9882	0,9951	0,9980	0,9992	0,9997	0,9999				
12,5	0,5824	0,8517	0,9441	0,9784	0,9917	0,9968	0,9988	0,9995	0,9998	0,9999				
13,0	0,6174	0,8734	0,9555	0,9841	0,9943	0,9980	0,9993	0,9997	0,9999	1,0000				
13,5	0,6509	0,8924	0,9648	0,9883	0,9961	0,9987	0,9996	0,9999	1,0000					
14,0	0,6812	0,9090	0,9724	0.9915	0,9973	0,9992	0,9998	0,9999						
14,5	0,7099	0,9234	0,9780	0.9938	0,9982	0,9995	0,9999	1,0000						
15,0	0,7367	0,9358	0,9833	0,9956	0,9988	0,9997	0,9999							
15,5	0,7615	0,9464	0,9872	0,9969	0,9992	0,9998	1,0000							
16,0	0,7844	0,9555	0,9902	0,9978	0,9995	0,9999								
16,5	0,8055	0,9631	0,9927	0,9985	0,9997	0,9999								
17,0	0,8249	0,9697	0,9944	0,9990	0,9998	1,0000								

17,5	0,8428	0,9752	0,9958	0,9993	0,9999								
18,0	0,8591	0,9797	0,9969	0,9995	0,9999								
18,5	0,8740	0,9836	0,9977	0,9997	1,0000								
19,0	0,8876	0,9867	0,9983	0,9998									
19,5	0,9000	0,9893	0,9988	0,9999									
20,0	0,9112	0,9915	0,9991	0,9999									
20,5	0,9213	0,9932	0,9994	0,9999									
21,0	0,9304	0,9946	0,9996	1,0000									
21,5	0,9386	0,9957	0,9997										
22,0	0,9460	0,9967	0,9998										
22,5	0,9526	0,9974	0,9998										
23,0	0,9590	0,9980	0,9999										
23,5	0,9636	0,9984	0,9999										
24,0	0,9696	0,9988	1,0000										
24,5	0,9724	0,9991											
25,0	0,9760	0,9993											
26	0,9821	0,9996											
27	0,9867	0,9998											
28	0,9902	0,9999											
29	0,9929	0,9999											
30	0,9949	1,0000											
35	0,9991												
40	0,9999												
43	1,0000												

Values of the function $L\left(y\sqrt{\frac{a}{1-a}}\right)$.

К ТЕОРИИ ВАРИАЦИОННЫХ РЯДОВ

А. РЕНЬИ (Будапешт)

(Резюме)

Цель настоящей статьи — изложение нового метода, с помощью которого можно простым и систематическим образом построить теорию вариационных рядов и доказать ряд новых теорем. Сущность метода состоит в том, что исследование предельных распределений величин, зависящих от членов вариационного ряда сводится к исследовании распределении функций от сумм независимых случайных величин. Этот метод исходит из факта, который первым заметил А. Н. Колмогоров в своей работе [6a], что члены вариационного ряда образуют цепь Маркова. Более того, как доказал S. Malmquist, если ξ_k^* $(k=1,2,\ldots,n)$—расположенные в возрастающем порядке члени элементов ξ_k $(k=1,2,\ldots,n)$ выборки объема n из статистической совокупности с непрерывной функцией распределение $F(x)$ и $\eta_k^* = F(\xi_k^*)$ $(k=1,2,\ldots,n)$, то величины $\left(\frac{\eta_k^*}{\eta_{k+1}^*}\right)^k$ $(k=1,2,\ldots,n)$ являются вполне независимыми и в интервале $(0,1)$ равномерно распределенными случайными величинами, и поэтому величини $\zeta_k = \log \eta_k^*$ образуют аддитивную цепь Маркова. Простое доказательство этого факта дано в § 1. § 2 содержит изложение применения этого факта к простого доказательства некоторых известных теорем теорий вариационных рядов. В § 3 сформулированы следующие новые результаты, полученные с помощью нового метода.

Пусть $F_n(x)$ означает эмпирическую функцию распределения выборки, т. е. положим $F_n(x) = \frac{k}{n}$ для $\xi_k^* \leq x < \xi_{k+1}^*$ $(k=1,2,\ldots,n-1)$, $F_n(x)=0$ для $x<\xi_1^*$ и $F_n(x)=1$ для $\xi_n^* \leq x$. Тогда имеем

Теорема 5.

$$\lim_{n\to\infty} \mathbf{P}\left(\sqrt{n} \sup_{0<a\leq F(x)\leq 1} \left\{\frac{F_n(x)-F(x)}{F(x)}\right\} < y\right) = \begin{cases} \sqrt{\frac{2}{\pi}} \int\limits_0^{y\sqrt{\frac{a}{1-a}}} e^{-\frac{t^2}{2}}\, dt & \text{для } y<0, \\ 0 & \text{для } y\leq 0. \end{cases}$$

Теорема 6.

$$\lim_{n\to\infty} \mathbf{P}\left(\sqrt{n} \sup_{0<a\leq F(x)\leq 1} \left|\frac{F_n(x)-F(x)}{F(x)}\right| < y\right) = \begin{cases} \frac{4}{\pi} \sum\limits_{k=0}^{\infty} (-1)^k \frac{e^{-\frac{(2k+1)^2 \pi^2 (1-a)}{8 y^2 a}}}{2k+1} & \text{для } y>0, \\ 0 & \text{для } y\leq 0. \end{cases}$$

Теорема 7.

$$\lim_{n\to\infty} \mathbf{P}\left(\sqrt{n} \sup_{0<a\leq F(x)\leq b\leq 1} \left\{\frac{F_n(x)-F(x)}{F(x)}\right\} < y\right) = \frac{1}{\pi} \int\limits_{-\infty}^{y\sqrt{\frac{b}{1-b}}} e^{-\frac{u^2}{2}} \left[\int\limits_0^{\left(\sqrt{\frac{b}{1-b}}y-u\right)\sqrt{\frac{a(1-b)}{b-a}}} e^{-\frac{t^2}{2}}\, dt \right] du$$

$$-\infty < y < +\infty.$$

Теорема 8.

$$\lim_{n\to 0} \mathbf{P}\left(\sqrt{n}_0 \sup_{a \leqq F(x) \leqq b-1} \left|\frac{F_n(x)-F(x)}{F(x)}\right| < y\right) = \frac{4}{\pi}\sum_{k=0}^{\infty}(-1)^k \frac{e^{-\frac{(2k+1)^2\pi^2(1-a)}{8y^2a}}}{2k+1} E_k$$

для $y \geqq 0$,

$$\text{где}\quad E_k = 1 - \frac{2}{\sqrt{2\pi}}\int_{y\sqrt{\frac{b}{1-b}}}^{\infty} e^{-\frac{u^2}{2}}\,du + \frac{2e^{-\frac{by^2}{2(1-b)}}}{\sqrt{2\pi\left(\frac{a}{1-a}\right)}\,y}\int_0^{(2k+1)\frac{\pi}{2}} e^{\frac{(1-b)u^2}{2by^2}}\sin u\,du.$$

Эти теоремы, которые аналогичны известным теоремам Н. В. Смирнова и А. Н. Колмогорова, дают критерии для гипотез относительно $F(x)$, соотв. дают доверительные границы для неизвестной функций $F(x)$.

Доказательство этих теорем содержится в § 5, и опирается, кроме упомянутого метода, на некоторых новых предельных теорем, изложенных в § 4, относительно максимума частных сумм последовательностей независимых случайних величин. § 6 содержит некоторые замечания относительно вычисления предельных функций распределения, фигурирующие в теоремах 5—8. В конце стати дана таблица значений функции

$$L(z) = \frac{4}{\pi}\sum_{k=0}^{\infty}(-1)^k e^{-\frac{(2k+1)^2\pi^2}{8z^2}} \quad \text{где} \quad z = y\sqrt{\frac{a}{1-a}}$$

для различных значений от y и a.

EINE BEMERKUNG ZUR KONVERGENZFRAGE DES LAGRANGESCHEN INTERPOLATIONSVERFAHRENS

Von

GEORG ALEXITS (Budapest), Mitglied der Akademie

1. Bezeichne $p(x) \geqq 0$ eine im endlichen Intervall $[a, b]$ definierte L-integrierbare Funktion. Sie bestimmt bekanntlich eindeutig ein System $\{P_n(x)\}$ von normierten Orthogonalpolynomen, wo $P_n(x)$ genau vom Grad n und der Koeffizient von x^n positiv ist. Wählen wir die Wurzeln $x_{n1}, x_{n2}, \ldots, x_{nn}$ von $P_n(x)$ als Grundpunkte der Lagrangeschen Interpolation und bezeichne

$$l_{nk}(x) = \frac{P_n(x)}{P_n'(x_k)(x - x_k)}$$

die n-te Grundfunktion, ferner

$$L_n(f, x) = \sum_{k=1}^{n} f(x_{nk}) l_{nk}(x)$$

das n-te Annäherungspolynom dieses Interpolationsverfahrens. Wir wollen im folgenden das Konvergenzproblem des Lagrangeschen Interpolationsverfahrens durch eine kurze Bemerkung vom Standpunkt der Theorie der Orthogonalpolynomentwicklungen erläutern.

2. Es ist bekannt, daß die Konvergenzfrage der Interpolationspolynome $L_n(f, x)$ engstens mit dem Problem der Größenordnung der Lebesgueschen Funktionen

$$\Lambda_n(x) = \sum_{k=1}^{n} |l_{nk}(x)|$$

zusammenhängt. Um diese zu untersuchen, setzen wir zunächst

$$\varepsilon_{nk}(x) = \operatorname{sign} l_{nk}(x),$$

ferner

$$Q_n(t, x) = \sum_{k=1}^{n} \varepsilon_{nk}(x) l_{nk}(t).$$

Bei festem x ist $Q_n(t, x)$ ein Polynom $(n-1)$-ten Grades in t und offensichtlich gilt $Q_n(t, x) = \Lambda_n(x)$, daher kann $\Lambda_n(x)$ in der Form

$$\Lambda_n(x) = \int_a^b p(t) Q_n(t, x) \sum_{k=0}^{n-1} P_k(t) P_k(x)\, dt$$

dargestellt werden. Daraus folgt durch Anwendung der Buniakowski—Schwartzschen Ungleichung:

$$[\Lambda_n(x)]^2 \leqq \int_a^b p(t)[Q_n(t,x)]^2\,dt \cdot \int_a^b p(t)\left[\sum_{k=0}^{n-1} P_k(t)P_k(x)\right]^2 dt.$$

Das erste dieser Integrale kann nach einem Resultat von GRÜNWALD und TURÁN[1] den Wert

$$C=\int_a^b p(t)\,dt$$

nicht übertreffen, wogegen das zweite den Wert $\sum_{k=0}^{n-1}[P_k(x)]^2$ hat. Folglich besteht die Abschätzung

$$\Lambda_n(x) \leqq \sqrt{C\sum_{k=0}^{n-1}[P_k(x)]^2}. \tag{1}$$

Aus dieser ergibt sich unschwer der folgende Satz:

Verschwindet $p(x)$ höchstens in den Punkten einer Nullmenge und erfüllt $f(x)$ in $[a,b]$ eine Lipschitzbedingung α-ter Ordnung mit $\alpha>\frac{1}{2}$, so konvergiert die Folge der Lagrangeschen Interpolationspolynome $L_n(f,x)$ in $[a,b]$ fast überall gegen $f(x)$.

Unser Satz folgt auf bekannte Weise, wenn es uns gelingt zu zeigen, daß in $[a,b]$ fast überall $\Lambda_n(x)=o(n^\alpha)$ besteht, was nach (1) mit der Behauptung gleichwertig ist, daß in $[a,b]$ fast überall die Abschätzung

$$\sum_{k=0}^{n-1}[P_k(x)]^2=o(n^{2\alpha}) \tag{2}$$

gilt. Wegen der Normiertheit des Systems $\{P_n(x)\}$ erhalten wir zunächst

$$\sum_{k=0}^{\infty}\int_a^b \frac{p(x)[P_k(x)]^2}{k(\log k)^{1+\varepsilon}}\,dx=\sum_{k=0}^{\infty}\frac{1}{k(\log k)^{1+\varepsilon}}<\infty.$$

Daraus folgt nach dem B. Levischen Satz[2] über Folgen L-integrierbarer Funktionen die Konvergenz in $[a,b]$ fast überall der aus den Integranden gebildeten Reihe, woraus sich nach einem oft gebrauchten Kroneckerschen Lemma[3] in $[a,b]$ fast überall

$$\sum_{k=0}^{n-1}p(x)[P_k(x)]^2=o(n(\log n)^{1+\varepsilon})$$

[1] G. GRÜNWALD und P. TURÁN, Über Interpolation, *Annali R. Scuola Normale Pisa*, (2), 7 (1938), S. 137—146.

[2] Vgl. F. RIESZ—B. SZ.-NAGY, *Leçons sur l'analyse fonctionnelle*, II. Aufl. (Budapest, 1953), S. 36.

[3] Vgl. A. ZYGMUND, *Trigonometrical series* (Warszawa—Lwów, 1935), S. 255.

ergibt. Da nach Annahme $p(x)$ höchstens in den Punkten einer Nullmenge verschwindet, kann man für fast alle x mit $p(x)$ dividieren, woraus man in $[a, b]$ fast überall

$$\sum_{k=0}^{n-1} [P_k(x)]^2 = o(n (\log n)^{1+\varepsilon})$$

erhält. Wegen $\alpha > \frac{1}{2}$ ist aber $n (\log n)^{1+\varepsilon} = o(n^{2\alpha})$, womit die Richtigkeit der Beziehung (2) und mithin auch unser Satz bewiesen ist.

2. Bemerkung. *Die Annahme, daß $p(x)$ nur auf einer Nullmenge verschwindet, ist mit der Vollständigkeit im Raume $L^2_{p(x)}$ des Polynomsystems $\{P_n(x)\}$ äquivalent.*

In der Tat, wäre $p(x) = 0$ in den Punkten einer Menge M von positivem Maß, so würden alle Entwicklungskoeffizienten der Funktion $f(x)$, welche in M identisch 1, sonst 0 ist, verschwinden, also könnte $\{P_n(x)\}$ in $L^2_{p(x)}$ nicht vollständig sein. — Sei nun umgekehrt $p(x) = 0$ höchtens in den Punkten einer Nullmenge. Dann ist mit dem System $\{x^n\}$ auch das System $\{\sqrt{p(x)}x^n\}$ vollständig im Raume L^2. Orthogonalisiert man das System $\{\sqrt{p(x)}x^n\}$ mittels des Schmidtschen Verfahrens, so ergibt sich das Orthogonalsystem $\{\sqrt{p(x)}P_n(x)\}$, welches somit in L^2 vollständig ist, also können für ein $g \in L^2$ und $g(x) > 0$ in einer Menge von positivem Maß nicht alle Momente

$$\mu_n = \int_a^b g(x)\sqrt{p(x)}P_n(x)dx$$

verschwinden. Ist nun $f(x)$ eine beliebige $L^2_{p(x)}$-integrierbare Funktion, die in einer Menge von positivem Maß von Null verschieden ist, so ist $g(x) = \sqrt{p(x)}f(x)$ eine L^2-integrierbare Funktion, daher können nicht alle Momente

$$\mu_n = \int_a^b p(x)f(x)P_n(x)\,dx$$

verschwinden, was eben die Vollständigkeit in $L^2_{p(x)}$ des Systems $\{P_n(x)\}$ bedeutet.

3. Shohat,[4] ferner Grünwald und Turán[1] haben den Satz bewiesen, daß $\{L_n(f(x)\}$ in jedem ganz im Inneren von $[a, b]$ liegenden Intervall I gleichmäßig gegen $f(x)$ konvergiert, wenn in $[a, b]$ die Beziehung $p(x) \geqq m > 0$ besteht und $f(x)$ eine Lipschitzbedingung α-ter Ordnung mit $\alpha > \frac{1}{2}$ erfüllt. Dieser Satz läßt sich — sogar in einer etwas verschärften, lokalisierten Form — aus der Abschätzung (1) herleiten:

Ist $[\alpha, \beta]$ ein beliebiges Teilintervall von $[a, b]$ und ist $p(x) \geqq m > 0$ in $[\alpha, \beta]$, genügt ferner $f(x)$ in $[a, b]$ einer Lipschitzbedingung α-ter Ordnung mit

[4] J. Shohat, On interpolation, *Annals of Mathematics*, (2), 34 (1933), S. 130—146.

$\alpha > \frac{1}{2}$, so konvergiert $\{L_n(f, x)\}$ in jedem ganz im Inneren von $[\alpha, \beta]$ liegenden Intervall I gleichmäßig gegen $f(x)$.

Unsere Behauptung ist ausgiebig bewiesen, wenn wir zeigen, daß in I gleichmäßig $\Lambda_n(x) = O(\sqrt{n})$ gilt. G. FREUD[5] hat aber aus $p(x) \geqq m > 0$ in $[\alpha, \beta]$ das gleichmäßige Bestehen der Abschätzung

$$\sum_{k=0}^{n-1} [P_k(x)]^2 = O(n)$$

in jedem ganz im Inneren von $[\alpha, \beta]$ liegenden Intervall I hergeleitet. Aus (1) folgt somit in I gleichmäßig $\Lambda_n(x) = O(\sqrt{n})$ und unsere Behauptung ist bewiesen.

(Eingegangen am 2. November 1953.)

[5] G. FREUD, Über die starke $(C, 1)$-Summierbarkeit von orthogonalen Polynomreihen, *Acta Mathematica Acad. Sci. Hung.*, **3** (1952), S. 83—88.

К ВОПРОСУ О СХОДИМОСТИ МЕТОДА ИНТЕРПОЛИРОВАНИЯ ЛАГРАНЖА

Г. АЛЕКСИЧ (Будапешт)

(Резюме)

Пусть $p(x) \geqq 0$ заданная в конечном промежутке $[a, b]$ L-интегрируемая функция. а $\{P_n(x)\}$ ортогональная система многочленов, определенная весом $p(x)$ однозначно Выберем в качестве узлов интерполирования Лагранжа корни $x_{n1}, x_{n2}, \ldots, x_{nn}$ многочлена $P_n(x)$ и обозначим через

$$L_n(f, x) = \sum_{k=1}^{n} f(x_{nk})\, l_{nk}(x)$$

n-ый полином Лагранжа, принадлежащий непрерывной в промежутке $[a, b]$ функции $f(x)$ сходимость которого как известно определяется порядком величины функций Лебега

$$\Lambda_n(x) = \sum_{k=1}^{n} |l_{nk}(x)|.$$

С помощью простой оценки этого последнего получаются следующие две теоремы:

1. Если $p(x) = 0$ не более, чем на множестве меры нуль, тогда $L_n(f, x)$ сходится к $f(x)$ почти всюду на отрезке $[a, b]$, если только $f \in \mathrm{Lip}\,\alpha$, где $\alpha > \frac{1}{2}$.

2. Если $p(x) \geqq m > 0$ и части $[\alpha, \beta]$ промежутка $[a, b]$ и $f(x)$ удовлетворяет в $[a, b]$ условию Липшица с показателем $\alpha > \frac{1}{2}$, тогда $L_n(f, x)$ сходится к $f(x)$ равномерно в каждом промежутке, целиком лежащем внутри $[\alpha, \beta]$.

Последний результат является несколько более острой локальной формой одной теоремы Шохата, Грюнвальда и Турана.

SUR UNE EQUATION DIFFERENTIELLE D'ORDRE n

Par

CHRISTO KARANICOLOFF (Sofia)

(*Présenté par* E. EGERVÁRY)

Nous nous proposons de donner une méthode pour déterminer au moins une solution — valable dans un voisinage du point singulier $z=0$ — de l'équation differentielle d'ordre $n(>1)$:

$$\frac{d^n w}{dz^n}=f(z,z^p)w; \tag{1}$$

p désigne une constante arbitraire positive; $f(z,u)$ est une fonction analytique de z et u dans les domaines:

$$G:\ |z|\leqq R; \quad G_1:\ |u|\leqq R_1=R^p. \tag{2}$$

($z^p=e^{p\log z}$ étant la valeur principale de $\log z$; R — constante positive.)

REMARQUE. Lorsque p est un nombre entier $\geqq 0$, le point $z=0$ n'est pas singulier et l'on peut résoudre l'équation (1) par les méthodes classiques, par exemple, celle de FROBENIUS [1]. C'est pourquoi nous supposerons que la constante p est une fraction ou bien un nombre irrationnel.

D'après nos hypothèses la fonction $f(z,u)$ peut être développée en série de la forme:

$$f(z,u)=\sum_{k=0}^{\infty} a_k(z)u^k \qquad (u=z^p), \tag{3}$$

valable pour chaque couple z, u de G, G_1.

En vertu des inégalités de CAUCHY

$$|a_k(z)|\leqq\frac{M}{R^k} \qquad (k=0,1,2,\dots)$$

nous avons pour chaque $z\in G$ et $u\in G_1$

$$|a_k(z)u^k|\leqq|a_k(z)|R_1^k\leqq M \qquad (k=0,1,2,\dots), \tag{4}$$

M étant le maximum de $|f(z,u)|$ lorsque u décrit la circonférence $|u|=R_1$.

On peut essayer de satisfaire à l'équation (1) en remplaçant w par une série de la forme

$$w(z)=\sum_{\nu=0}^{\infty} c_\nu(z)z^{p\nu}. \tag{5}$$

En égalant les coefficients de $z^{p\nu}$ $(\nu=0, 1, 2, \ldots)$ dans les deux membres de (1) on obtient le système d'équations suivant:

$$(A)\qquad \begin{cases} c_0^{(n)} = a_0 c_0 \\ (c_1 z^p)^{(n)} = (a_0 c_1 + a_1 c_0) z^p \\ (c_2 z^{2p})^{(n)} = (a_0 c_2 + a_1 c_1 + a_2 c_0) z^{2p} \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ (c_k z^{pk})^{(n)} = (a_0 c_k + a_1 c_{k-1} + \cdots + a_k c_0) z^{pk} \end{cases}$$

pour la détermination des inconnues $c_\nu(z)$.

Si nous divisons par $z^{pk}(k=0, 1, 2, \ldots)$ les équations du système (A), nous obtenons des équations du type fuchsien et par conséquent on connaît les méthodes de leur résolution [2]. Il faudrait ensuite étudier la convergence de la série (5), ce qu'on ne peut pas voir directement.

Pour résoudre cette question nous procédons de la façon suivante:

1. Nous choisirons deux constantes arbitraires positives r et ϱ satisfaisant aux conditions:

$$(6)\qquad r = R_1 \frac{\varrho}{2} < \frac{R_1}{2} \qquad (0<\varrho<1).$$

2. Nous donnerons aux équations (A) la forme suivante:

$$(7)\qquad \begin{cases} c_0^{(n)} = a_0 c_0 \\ (c_k z^{pk})^{(n)} = a_0 c_k z^{pk} + F_k \\ F_k = (a_1 c_{k-1} + a_2 c_{k-2} + \cdots + a_k c_0) z^{pk} \end{cases} \Big\} k = 1, 2, 3, \ldots$$

et poserons

$$c_k z^{pk} = u_k \qquad (k=0, 1, 2, \ldots)$$

ce qui conduit aux équations

$$(8)\qquad u_k^{(n)} = a_0(z) u_k + F_k \qquad (k=0, 1, 2, \ldots;\ F_0 \equiv 0).$$

L'équation (8) est une équation linéaire en u_k avec second membre (F_k). Nous pouvons déterminer n intégrales particulières: $U_1(z), U_2(z), \ldots, U_n(z)$ — linéairement indépendantes — de l'équation homogène

$$(9)\qquad u^{(n)} = a_0(z) u$$

et par conséquent

$$u_k = u + v_k;\quad u = \sum_{\lambda=1}^{n} C_\lambda U_\lambda(z) \qquad (C_\lambda \text{— des const. arbitraires}),$$

v_k étant une intégrale particulière de l'équation (8).

On peut déterminer v_k par la méthode de Lagrange en posant:

$$(10)\qquad v_k = \varphi_{k1}(z) U_1(z) + \varphi_{k2}(z) U_2(z) + \cdots + \varphi_{kn}(z) U_n(z).$$

Ainsi nous obtenons l'équation:

$$(11)\qquad v_k(z) = \frac{1}{\Delta} \sum_{\lambda=1}^{n} U_\lambda(z) \int_0^z \Delta_{k\lambda}(t) dt \qquad (k=1, 2, 3, \ldots)$$

dans laquelle:

1. Δ désigne le déterminant de WRONSKI:

$$\Delta(z) = \begin{vmatrix} U_1(z) \cdots U_n(z) \\ U_1' \quad \cdots U_n' \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ U_1^{(n-1)} \cdots U_n^{(n-1)} \end{vmatrix}$$

qui est égal à une constante $\Delta \neq 0$, car le coefficient de $U^{(n-1)}$ dans (9) est égal à zéro et les fonctions: $U_1, U_2, \ldots, U_n$ sont linéairement indépendantes;

2. $\Delta_{k\lambda}(t)$ désigne le déterminant obtenu en remplaçant dans $\Delta(t)$ les éléments de la λ-ième colonne par: $0, 0, \ldots, F_k$ $(k=1, 2, 3, \ldots; \lambda=1, 2, \ldots, n)$;

3. les intégrales (11) sont prises sur le segment:

$$t=0,\ t=z;\ z \in K.$$

4. On sait que les intégrales $U_1(z), U_2(z), \ldots, U_n(z)$ de l'équation (9) sont des fonctions holomorphes de z dans le cercle de centre l'origine 0 et de rayon R' égal à la distance de 0 au point singulier de $a_0(z)$ le plus rapproché de 0. Par conséquent la région K ci-dessus est l'intérieur du cercle $<R'$ avec la coupure rectiligne joignant les points $z=0$ et $z=-R'$.

Donc, on aura la solution suivante du système (7) ou (A):

$$(12) \qquad c_k z^{pk} = \varrho^k U_1(z) + \frac{1}{\Delta} \sum_{\lambda=1}^{n} U_\lambda(z) \cdot \int_0^z \Delta_{k\lambda}(t)\,dt \qquad (k=0, 1, 2, \ldots)$$

$(\Delta_{01} = \Delta_{02} = \ldots = \Delta_{0n} = 0$, car $F_0 \equiv 0)$.

(On sait que si $U_1(z)$ est une solution de l'équation (9), la fonction $CU_1(z)$ est aussi une solution de la même équation. Dans la formule (12) nous avons choisi pour la constante C la valeur spéciale: ϱ^k.)

Comme les fonctions: $U_1(z), U_2(z), \ldots, U_n(z)$ sont holomorphes dans le cercle $|z|<R'$, on peut affirmer que dans la région $|z| \leqq R'' < R'$ elles-mêmes et leurs dérivées d'ordre μ $(\mu=0, 1, 2, \ldots, n-2)$ sont bornées:

$$(13) \qquad |U_\nu(z)^{(\mu)}| \leqq P \quad (P>0;\ \mu=0, 1, \ldots, n-2;\ \nu=1, 2, \ldots, n)$$

$$(14) \qquad |U_1(z)| = |c_0(z)| < \frac{N}{s} < N$$

$(N>0;\ s>1;\ s$ sera choisi convenablement).

Nous désignons ensuite par δ un nombre positif qui est soumis aux conditions:

$$(15) \qquad \delta < \frac{|\Delta|}{M \cdot P^n \cdot n\sqrt{(n-1)^{n-1}}},$$

$$(16) \qquad \delta \leqq \min(R'', r^{1/p})$$

et par L le domaine circulaire $|z|<\delta$ qui est coupé suivant le segment: $z=0, z=-\delta$.

Toutes ces hypothèses admises, nous allons démontrer la convergence de la série (5) pour chaque valeur de z appartenant au domaine L.

Dans ce but nous allons nous baser sur la méthode de l'induction mathématique et nous montrerons pour chaque z de la région L la validité des inégalités

(17) $$|c_k z^{pk}| < N\varrho^k \qquad (k = 0, 1, 2, 3, \ldots).$$

D'abord, il est évident que l'inégalité (17) a lieu pour $k=0$, parce que dans ce cas elle est identique à (14).

En supposant que l'inégalité (17) est vérifiée pour $k=0, 1, 2, \ldots, m-1$, il faut prouver qu'elle est également vraie aussi pour $k=m$. Çependant, il est nécessaire dans ce but d'établir au préalable l'exactitude d'une inégalité auxiliaire (v. (19)).

On déduit de (4) et (6):

$$|a_k(z) z^{pk}| \leqq |a_k(z)| \cdot \left(\frac{2r}{\varrho}\right)^k \leqq M$$

ou bien (lorsque z appartient à la région $|z| < r^{1/p}$ et par conséquent à la région L):

(18) $$|a_k(z)| r^k \leqq M\left(\frac{\varrho}{2}\right)^k.$$

De même, pour chaque z de la région L, on a:

$$|a_k(z) z^{pk}| \leqq |a_k(z)| r^k$$

ou bien, en vertu de (18), on déduit:

(19) $$|a_k(z) z^{pk}| \leqq M \cdot \left(\frac{\varrho}{2}\right)^k$$

ce qui représente l'inégalité auxiliaire désirée.

Enfin, en nous servant des inégalités (13) et (19) nous obtenons (pour chaque z de la région K et par conséquent de L):

(20) $$|\varDelta_{k\nu}(z)| \leqq M \cdot N \cdot P^{n-1} \sqrt{(n-1)^{n-1}} \left(\frac{1}{2} + \frac{1}{2^2} + \cdots + \frac{1}{2^k}\right) \cdot \varrho^k < ^{*}$$
$$< M \cdot N \cdot P^{n-1} \cdot \sqrt{(n-1)^{n-1}} \cdot \varrho^k; \qquad k = 1, 2, \ldots, m; \; \nu = 1, 2, \ldots, n.$$

Il s'ensuit de (20) et (12) que

$$|c_m z^{mp}| \leqq |\varrho^m \cdot U_1(z)| + \frac{1}{|\varDelta|} \cdot \sum_{\nu=1}^{n} |U_\nu(z)| \cdot \left|\int_0^z \varDelta_{m\nu}(t)\, dt\right| \qquad (m = 0, 1, 2, \ldots)$$

ou bien (d'après (14)):

(21) $$|c_m z^{mp}| < \varrho^m \cdot N \cdot \left[\frac{1}{s} + \frac{M \cdot P^n \cdot n \cdot \sqrt{(n-1)^{n-1}}}{|\varDelta|}\, \delta\right].$$

* D'après l'inégalité bien connue de M. Hadamard sur les déterminants

Mais, suivant notre hypothèses pour δ [(15)], il est toujours possible de choisir le nombre $s(>1)$ de sorte que l'on ait:

$$\frac{1}{s}+\frac{M\cdot P^n n\sqrt{(n-1)^{n-1}}}{|\Delta|}\delta=1.$$

Le nombre s défini, l'inégalité (21) devient:

$$|c_m z^{mp}|<N\cdot\varrho^m \qquad (0<\varrho<1),$$

et elle a lieu pour chaque valeur de z, appartenant à L et pour $m=0,1,2,\ldots.$ Mais tout celą démontre que la série (5) est uniformément convergente pour chaque z de L, c. q. f. d.

D'une façon analogue on peut résoudre dans un certain voisinage du point singulier $z=0$ des équations différentielles de la forme:

$$\frac{d^n w}{dz^n}+\sum_{\nu=1}^{n} f_\nu(z,z^p)\cdot\frac{d^{n-\nu}w}{dz^{n-\nu}}=0 \qquad (n>1)$$

($p>0$; $f_\nu(z,u)$ étant des fonctions analytiques par rapport à z et par rapport à u dans deux domaines, contenant resp. le point $z=0$ et $u=0$).

REMARQUE. On démontre facilement que les fonctions $c_\nu(z)z^{p\nu}$ sont holomorphes dans la région L. On en déduit (d'après un théorème classique de WEIERSTRASS) que la série (5) peut être différentiée — ce que nous avons déjà fait pour écrire le système (A).

(Reçu le 9 avril 1952.)

Littérature

[1] E. INCE, *Ordinary differential equations* (New York, 1944).
[2] L. FUCHS, *Journal für reine u. angew. Math.*, **66** (1866).

ОБ ОДНОМ ДИФФЕРЕНЦИАЛЬНОМ УРАВНЕНИЙ n-ОГО ПОРЯДКА

ХР. КАРАНИКОЛОВ (София)

(Резюме)

В настоящем работе автор даёт метод для нахождения хотя одного решения следующего уравнения:

(1) $$\frac{d^n w}{dz^n}=f(z, z^p)w,$$

где p означает одну положителную константу; $f(z, u)$ — аналитическая функция от z и u в областях:

(2) $$G\colon |z|\leq R;\ G_1\colon\ |u|\leq R_1=R^p\quad (u=z^p;\ R>0).$$

Решение имеет вид:

$$w=\sum_{\nu=0}^{\infty} c_\nu(z)z^{p\nu}$$

и является аналитическую функцию в некотором круге вокруг точки $z=0$.

ÜBER DIE HILBERTSCHE BEGRÜNDUNG DER HYPERBOLISCHEN GEOMETRIE

Von

PAUL SZÁSZ (Budapest)

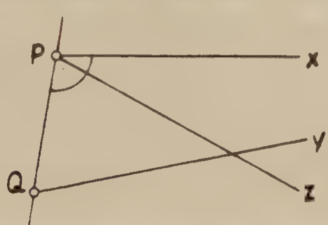
(*Vorgelegt von* G. HAJÓS)

D. HILBERT[1] hat bei seiner neuen Begründung der hyperbolischen Geometrie der Ebene auf die Stetigkeitsaxiome verzichtet, und die Existenz der hyperbolischen Parallelen, die durch einen Punkt zu einer Geraden gelegt werden können, als Axiom vorausgesetzt.[2] Nach seiner Erklärung bestimmt jede Halbgerade ein *Ende*; von allen Halbgeraden, die zueinander hyperbolisch parallel sind, sagt man, daß sie dasselbe Ende bestimmen. Die Enden sind also mit anderen Worten die *unendlich fernen Punkte* der Ebene. Auf Grund des genannten Axioms, besitzt eine Gerade stets zwei Enden. Nach dem Beweis einiger grundlegenden Tatsachen der hyperbolischen Ebene, definiert D. HILBERT[3] nach beliebiger Wahl der Enden $0, 1, \infty$ die Addition und

[1] D. HILBERT, Neue Begründung der Bolyai—Lobatschefskyschen Geometrie, *Mathematische Annalen*, 57 (1903), S. 137—150, oder *Grundlagen der Geometrie*, 7. Aufl. (Leipzig und Berlin, 1930), Anhang III. S. 159—177.

[2] Es sei hier bemerkt, daß dieses Axiom IV von D. HILBERT (a. a. O., S. 139—140 bzw. S. 162) durch eine schwächere Voraussetzung ersetzt werden kann, die in den nachstehenden zwei Axiomen ihren Ausdruck findet.

IV_1. *Es seien P, Q zwei verschiedene Punkte in der Ebene und QY eine Halbgerade an der einen Seite der Geraden PQ. So gibt es stets eine Halbgerade PX an derselben Seite von PQ, die QY nicht schneidet, während jede im $\sphericalangle QPX$ gelegene innere Halbgerade PZ die Halbgerade QY schneidet* (siehe die beigelegte Figur).



IV_2. *Es gibt eine Gerade g_0 und einen nicht auf ihr liegenden Punkt P_0 der Ebene derart, daß durch P_0 zwei verschiedene Geraden gelegt werden können, die g_0 nicht schneiden.*

[3] D. HILBERT, a. a. O.[1], §§ 2—3.

Multiplikation der Enden und gelangt zum Ergebnis, daß für die Rechnung mit Enden die nämlichen Regeln gelten wie für die Rechnung mit gewöhnlichen Zahlen. Er schließt seine Abhandlung mit folgenden Worten:

„Nachdem wir erkannt haben, daß die Gleichung des Punktes in Linienkoordinaten eine lineare ist, folgern wir leicht den speziellen Pascalschen Satz für das Geradenpaar und den Desarguesschen Satz über perspektiv liegende Dreiecke sowie die übrigen Sätze der projektiven Geometrie. Auch sind dann die bekannten Formeln der Bolyai—Lobatschefskyschen Geometrie ohne Schwierigkeit ableitbar, und damit ist der Aufbau dieser Geometrie mit alleiniger Hilfe der Axiome I—IV vollendet."

In vorliegender Note wird nun in aller Kürze gezeigt, daß bei dieser Vollendung die projektive Geometrie vermieden und der Aufbau mit ganz elementaren Hilfsmitteln durchgeführt werden kann. Zu diesem Zwecke wird zunächst die Äquivalenz der hyperbolischen Geometrie der Ebene mit der bekannten Bildgeometrie von H. POINCARÉ[4] auf der euklidischen Halbebene erwiesen,[5] und sodann die Herleitung der von der Stetigkeit unabhängigen Grundgleichungen der hyperbolischen Ebene angedeutet.

§ 1. Die Äquivalenz der hyperbolischen Geometrie der Ebene mit der Poincaréschen Bildgeometrie

Aus dem Körper der Enden werde eine euklidische Ebene konstruiert, deren *„Punkte"* also die Paare (α, β) sind, wobei α und β je ein beliebiges (von ∞ verschiedenes) Ende bedeuten. In dieser euklidischen Ebene gilt außer der Hilbertschen Axiomgruppen I, II, III und dem euklidischen Parallelenaxiom auch das *Kreisaxiom,*[6] da doch im Körper der Enden die Quadratwurzel eines jeden positiven Endes existiert.

Die hyperbolische Ebene sei nun eineindeutig auf die euklidische Halbebene $\beta > 0$ abgebildet, und zwar in folgender Weise.

[4] Vgl. H. POINCARÉ, Théorie des groupes fuchsiens, *Acta Mathematica,* **1** (1882), S. 1—62, besonders § 2, S. 6—8. Da wir auf die Stetigkeitsaxiome verzichten, so muß auf der zugrunde gelegten euklidischen Ebene auch das *Kreisaxiom* vorausgesetzt werden, laut welchem *irgendein Kreis von jeder Geraden geschnitten wird, der einen Punkt im Innern dieses Kreises hat.* Übrigens kann diese Bildgeometrie in trivialer Weise vollständig elementar dargestellt werden, ohne Benützung komplexer Größen.

[5] Ganz anders geht zuwerke B. KERÉKJÁRTÓ, A hiperbolikus síkgeometria felépítése (ungarisch), *Matematikai és Természettudományi Értesitő,* **59** (1940), S. 19—59, oder Nouvelle méthode d'édifier la géométrie plane de Bolyai et de Lobatchefski, *Commentarii Mathematici Helvetici,* **13** (1940), S. 11—48. Hier wird geradezu die Identität der hyperbolischen Geometrie der Ebene mit der Poincaréschen Bildgeometrie einer, auf der hyperbolischen Ebene selbst gedeuteten euklidischen Halbebene bewiesen, auch ohne Annahme von Stetigkeitsaxiomen.

[6] Siehe unter Fußnote [4]. Infolgedessen nehmen die Winkelfunktionen $\sin x$ und $\cos x$ (die auf Grund der Hilbertschen Streckenrechnung euklidisch erklärt werden können) jeden Wert an, der seinem Betrage nach ≤ 1 ist.

Ein jeder Punkt P der hyperbolischen Ebene kann durch eine Gleichung

$$(\mu\xi+\lambda)(\mu\eta+\lambda)=-1 \qquad (\mu>0) \tag{1}$$

charakterisiert werden,[7] wobei ξ, η die Enden einer beliebigen, durch P gelegten Geraden bedeuten, ausgenommen natürlich diejenige Gerade, die P mit dem unendlich fernen Punkt ∞ verbindet. Der Schnittpunkt O der beiden Geraden mit den Enden $0, \infty$ bzw. $-1, 1$ wird speziell durch die Gleichung $\xi\eta=-1$ charakterisiert. Umgekehrt ist durch eine Gleichung von der Form (1), bei beliebiger Wahl von $\mu>0$ und λ, stets ein Punkt charakterisiert. Werden aber in der euklidischen Halbebene $\beta>0$ über jede Strecke, die zwei Punkte $(\xi, 0), (\eta, 0)$ der Abszissenachse verbindet, Halbkreise geschlagen, so sind mit der Gleichung (1) diejenigen Halbkreise charakterisiert, die durch den Punkt $\left(-\frac{\lambda}{\mu}, \frac{1}{\mu}\right)$ dieser Halbebene hindurchgehen. Das erhellt aus dem Umstand, daß die durch den Punkt $(0, 1)$ gehenden Halbkreise offenbar durch die Gleichung $\xi\eta=-1$ charakterisiert sind. Werden nämlich die Streckung in Bezug auf den Ursprung $(0,0)$

$$\alpha'=\mu\alpha, \quad \beta'=\mu\beta,$$

und die Parallelverschiebung längs der Abszissenachse

$$\alpha'=\alpha+\lambda, \quad \beta'=\beta,$$

nacheinander ausgeführt, so geht dieser Punkt $\left(-\frac{\lambda}{\mu}, \frac{1}{\mu}\right)$ in $(0, 1)$, und die Gesamtheit der die Abszissenachse orthogonal schneidenden Halbkreise in sich selbst über. Die geplante Abbildung der hyperbolischen Ebene auf die euklidische Halbebene $\beta>0$ besteht nunmehr darin, daß wir den Punkt P mit der Gleichung (1) auf den Schnittpunkt derjenigen Halbkreise abbilden, die ebenfalls durch (1) charakterisiert sind, d. h. auf den Punkt $\left(-\frac{\lambda}{\mu}, \frac{1}{\mu}\right)$.

Das Bild einer Geraden mit den Enden ξ, η ist offenbar ein Halbkreis, der über die Punkte $(\xi, 0), (\eta, 0)$ verbindende Strecke geschlagen wird. Die durch den unendlich fernen Punkt ∞ gehenden Geraden werden auf die oberen Hälften derjenigen Geraden abgebildet, die mit der Ordinatenachse parallel sind. Das leuchtet ein, wenn man bedenkt, daß $-\frac{\lambda}{\mu}$ das andere Ende derjenigen Geraden ist, die den Punkt (1) mit ∞ verbindet.

[7] Vgl. D. Hilbert, a. a. O. [1], § 4. Die Einführung der Linienkoordinaten

$$u=\xi\eta, \quad v=\frac{\xi+\eta}{2}$$

hat bei D. Hilbert den Zweck, die Gleichung zu einer linearen zu machen. Für unsere Zwecke ist das unnötig.

Die Bewegungen bzw. Umlegungen der hyperbolischen Ebene sind, auf die Enden ξ bezogen, analytisch durch die linearen Transformationen

$$\xi' = \frac{\alpha\xi+\beta}{\gamma\xi+\delta}, \qquad \alpha\delta-\beta\gamma>0, \tag{2}$$

bzw.

$$\xi' = \frac{\alpha\xi+\beta}{\gamma\xi+\delta}, \qquad \alpha\delta-\beta\gamma<0 \tag{3}$$

dargestellt. Da nämlich die Transformationen

$$\xi = \xi+\lambda, \quad \xi' = -\frac{1}{\xi}, \quad \xi' = \mu\xi \quad (\mu>0)$$

der Reihe nach eine Drehung um den unendlich fernen Punkt ∞, die Halbdrehung um den Punkt O, eine Verschiebung längs der Geraden mit den Enden 0 und ∞ bedeuten, so stellt die Transformation (2) auf Grund der Umformung (im Falle $\gamma \neq 0$)

$$\frac{\alpha\xi+\beta}{\gamma\xi+\delta} = \frac{\alpha}{\gamma} + \frac{\alpha\delta-\beta\gamma}{\gamma^2} \frac{-1}{\xi+\dfrac{\delta}{\gamma}}$$

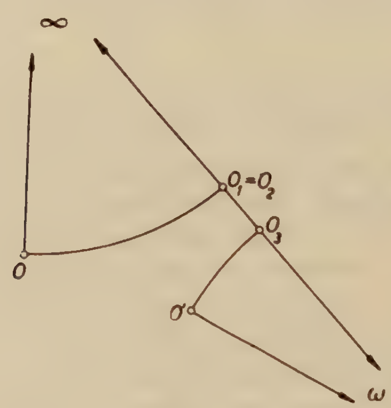


Fig. 1.

eine Bewegung der hyperbolischen Ebene dar (das leuchtet unmittelbar ein, falls $\gamma=0$ ist). Umgekehrt kann eine jede Bewegung der hyperbolischen Ebene durch eine derartige Transformation dargestellt werden, wie es die folgende Überlegung[8] zeigt. Die Bewegung ist durch die Angabe derjenigen Halbgeraden $O'\omega$, die in $O\infty$ übergeführt wird (Fig. 1), vollkommen bestimmt. Ist $\omega \neq \infty$, und wird die Gerade mit den Enden ω, ∞ vom Grenzkreis

[8] Vgl. P. Szász, Neue Bestimmung des Parallelwinkels in der hyperbolischen Ebene mit den klassischen Hilfsmitteln, *Acta Scientiarum Mathematicarum* (Szeged), **14** (1952), S. 247—251, besonders S. 249.

durch O mit dem Mittelpunkt ∞ in $O_1 = O_2$, von dem durch O' mit dem Mittelpunkt ω in O_3 geschnitten, so führt eine Drehung um ∞ die Halbgerade $O_1\infty$ in $O\infty$, die Halbdrehung um $O_1 = O_2$ die Halbgerade $O_2\omega$, in $O_1\infty$, eine Verschiebung längs der ω mit ∞ verbindenden Geraden $O_3\omega$ in $O_2\omega$, endlich eine Drehung um ω die Halbgerade $O'\omega$ in $O_3\omega$ über. Geht also ein Ende ξ bei der betrachteten Bewegung (die $O'\omega$ in $O\infty$ überführt) in ξ' und bei denjenigen, die $O_1\infty, O_2\omega, O_3\omega$ in $O\infty$ überführen, der Reihe nach in ξ_1, ξ_2, ξ_3 über, so ist offenbar

$$\xi_1 = \xi + \lambda, \quad \xi_2 = -\frac{1}{\xi_1}, \quad \xi_3 = \mu\xi_2 \quad (\mu > 0), \quad \xi' = \xi_3 + \nu,$$

wobei λ, μ, ν von ξ unabhängig sind. Folglich ist die betrachtete Bewegung durch eine Transformation

$$\xi' = -\frac{\mu}{\xi+\lambda} + \nu = \frac{\nu\xi + \nu\lambda - \mu}{\xi + \lambda} \qquad (\mu > 0)$$

dargestellt, die die Form (2) hat. (Im Falle $\omega = \infty$ ist die Bewegung eine Drehung um ∞, also durch eine Transformation $\xi' = \xi + \lambda$ darstellbar.) Die Transformation $\xi' = -\xi$ stellt offenbar die Spiegelung an der Geraden mit den Enden $0, \infty$ dar, also bedeuten die Transformationen (3), auf Grund der Bedeutung der Transformationen (2), die Umlegungen der hyperbolischen Ebene. Diese Transformationen (2) bzw. (3) bestimmen andererseits, auf die Abszissen ξ bezogen, eben die Bewegungen resp. Umlegungen in der Poincaréschen Bildgeometrie[9] auf der euklidischen Halbebene $\beta > 0$. Daraus geht schon hervor, daß bei der obigen Abbildung gleiche Winkel in ebenfalls gleiche Winkel übergehen, die gleichsinnig oder ungleichsinnig sind, je nachdem die ursprünglichen gleichsinnig oder ungleichsinnig ausfallen.

Damit ist die Äquivalenz der hyperbolischen Geometrie der Ebene mit der Poincaréschen Bildgeometrie erwiesen.

§ 2. Die von der Stetigkeit unabhängigen Grundgleichungen der hyperbolischen Ebene

Es sei in der obigen Abbildung das Bild eines jeden Punktes sowie eines jeden Winkels mit demselben Buchstaben bezeichnet. *Die trigonometrischen Funktionen eines Winkels sollen definitionsgemäß die euklidisch definierten trigonometrischen Funktionen seines Bildes bedeuten.* Wird durch den Schnittpunkt O der Geraden mit den Enden $0, \infty$ bzw. $-1, 1$ eine Gerade gelegt, deren Enden $\xi > 0$ und η sind (Fig. 2), so gilt für den Winkel

$$\tau = \sphericalangle \xi O \infty$$

[9] Vgl. Fußnote [4].

die Formel

$$\operatorname{ctg}\frac{\tau}{2} = \xi. \tag{4}$$

Das ist an unserer Abbildung unmittelbar abzulesen, da doch in der euklidischen Halbebene $\sphericalangle O\xi 0 = \frac{\tau}{2}$ ausfällt (Fig. 3). Die dem Winkel τ entsprechende Paralleldistanz $\overline{OS}$ (Fig. 2) werde mit t bezeichnet und es sei

$$\xi = E(t) \tag{5}$$

gesetzt. Diese Funktion genügt mit Rücksicht auf die Definition der Multiplikation der Enden [10] der Funktionalgleichung

$$E(t_1 + t_2) = E(t_1)E(t_2). \tag{6}$$

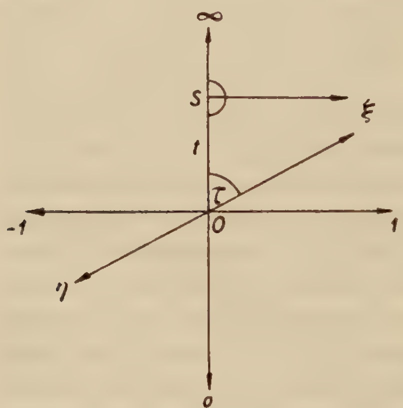


Fig. 2.

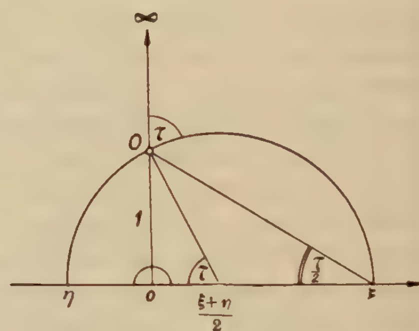


Fig. 3.

(Die Paralleldistanz t wird positiv oder negativ genommen, je nachdem $\sphericalangle \xi O \infty$ spitz oder stumpf ist.) Zwischen dem Abstand t und dem Parallelwinkel τ besteht nach (4) und (5) die fundamentale Beziehung

$$\operatorname{ctg}\frac{\tau}{2} = E(t). \tag{7}$$

Diese Formel kann gleich verallgemeinert werden. Zieht man nämlich von den Endpunkten des Abstandes $t = \overline{OS}$ irgend zwei Halbgeraden $O\xi, S\xi$ mit demselben Ende $\xi > 0$ (Fig. 4) und wird

$$\sphericalangle \xi OS = \omega, \quad \sphericalangle OS\xi = \sigma$$

gesetzt, so folgt aus (6) und (7) allgemeiner

$$\operatorname{ctg}\frac{\omega}{2}\operatorname{ctg}\frac{\sigma}{2} = E(t). \tag{8}$$

[10] D. HILBERT, a. a. O.[1], § 3.

Für ein rechtwinkliges Dreieck ABC ($\sphericalangle C$ ein rechter) mit den Bestimmungstücken

$$\overline{BC}=a, \quad \overline{CA}=b, \quad \overline{AB}=c, \quad \sphericalangle BAC=A, \quad \sphericalangle CBA=B$$

kann man nun, einem eleganten Gedankengang von J. HJELMSLEV[11] folgend, mit Hilfe der Formel (8) die nachstehenden Grundgleichungen herleiten. Werden der Kürze wegen außer der Streckenfunktion (5) noch die Streckenfunktionen

$$(9) \qquad C(t)=\frac{E(t)+E(-t)}{2}, \quad S(t)=\frac{E(t)-E(-t)}{2}, \quad T(t)=\frac{S(t)}{C(t)}$$

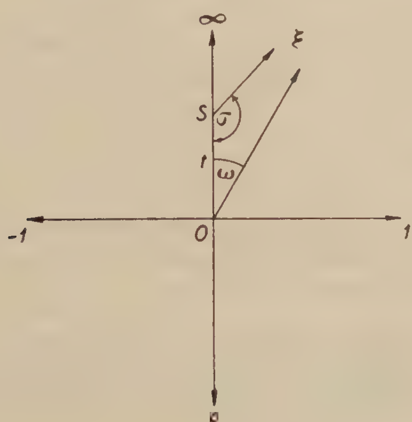


Fig. 4.

eingeführt, so lauten diese Gleichungen

$$(\mathrm{I}) \qquad \sin A=\frac{S(a)}{S(c)},$$

$$(\mathrm{II}) \qquad C(c)=\operatorname{ctg} A \operatorname{ctg} B,$$

$$(\mathrm{III}) \qquad C(c)=C(a)\,C(b).$$

Aus diesen folgen noch

$$(\mathrm{IV}) \qquad C(a)=\frac{\cos A}{\sin B},$$

$$(\mathrm{V}) \qquad \cos A=\frac{T(b)}{T(c)},$$

$$(\mathrm{VI}) \qquad \operatorname{tg} A=\frac{T(a)}{S(b)}.$$

Hierbei bedeuten (wir wiederholen es) die Winkelfunktionen die euklidisch

[11] J. HJELMSLEV, *Grundlag for den projektive Geometri* (Kobenhavn, 1943), besonders § 7, S. 36—37.

definierten trigonometrischen Funktionen der Bilder der Winkel A, B bei der obigen Abbildung der hyperbolischen Ebene auf die euklidische Halbebene. Die vorkommenden Streckenfunktionen, die unter (9) definiert wurden, stehen sich auf Grund der Funktionalgleichung (6) in vollständiger Analogie mit den Hyperbelfunktionen $\operatorname{ch} x$, $\operatorname{sh} x$, $\operatorname{th} x$.

(*Eingegangen am 7. April 1953.*)

О ГИЛЬБЕРТОВСКОМ ОБОСНОВАНИИ ГИПЕРБОЛИЧЕСКОЙ ГЕОМЕТРИИ

П. САС (Будапешт)

(Резюме)

В настоящей статье плоская гиперболическая геометрия строится на гильбертовой основе совершенно элементарными средствами, независимо от непрерывности и без привлечения проективной геометрии, на котором Гильберт ссылается в конце своей работы.

Рассматривается эвклидова плоскость, конструированная из тела, состоящего из концов, „точками“ которой являются следовательно двойки (α, β), где α и β произвольные отличные от ∞ концы. Отображаем гиперболическую плоскость в эвклидову полуплоскость $\beta > 0$, так, что точке P, заданной уравнением

$$(\mu\xi + \lambda)(\mu\eta + \lambda) = -1 \qquad (\mu > 0)$$

поставим в соответствие точку $\left(-\frac{\lambda}{\mu}, \frac{1}{\mu}\right)$ упомянутой полуплоскости. Здесь ξ и η концы произвольных прямых, проходящих через P (исключая конечно прямую с концам в бесконечности). При этом плоская гиперболическая геометрия изображается в эвклидовой полуплоскости картиной Пуанкаре.

С помощью этого изображения мы выводим основную формулу, из которой можно получить независимые от непрерывности основные уравнения гиперболической плоскости применением одного изящного рассуждения, принадлежащего И. Хьелмслеву. Поэтому достаточно их перечислить. В этих формулах тригонометрические функции данного угла означают обыкновенные тригонометрические функции угла, изображающего данное на картине Пуанкаре, а фигурирующие там функции расстояния являются аналогами гиперболических функций.

ÜBER DIE REKTIFIKATION DES KREISES, DES GRENZKREISES UND DER ABSTANDSLINIE

Von

PAUL SZÁSZ (Budapest)

(*Vorgelegt von* G. HAJÓS)

In einer früheren Arbeit[1] haben wir die beiden nachstehenden Sätze unabhängig vom Parallelenaxiom bewiesen.

SATZ I. *Sind die Winkel $\sigma > \sigma'$ Zentriwinkel im Kreise mit den entsprechenden Sehnen s und s', so besteht die Ungleichung*

$$\frac{\sigma'}{\sigma} < \frac{s'}{s}.$$

Eine Folge dieses Satzes war der

SATZ II. *Bezeichnet σ bzw. s die Maßzahl eines Zentriwinkels im Kreise bzw. der entsprechenden Sehne, so strebt das Verhältnis $s:\sigma$ für $\sigma \to 0$ einem bestimmten positiven Grenzwert zu.* (Der natürlich von der Wahl der Einheiten abhängt.)

Dieser Grenzwert ist eine Funktion des Kreishalbmessers r und soll mit $K(r)$ bezeichnet werden. Diese Streckenfunktion ist also durch die Formel

$$K(r) = \lim \frac{s}{\sigma} \qquad (\sigma \to 0)$$

erklärt, wobei σ die Maßzahl eines Zentriwinkels im Kreise mit dem Radius r und s die entsprechende Sehne bedeutet.[2]

Im Besitze dieser Streckenfunktion $K(r)$ können wir nun sogleich den Hauptsatz der Kreismessung beweisen, nämlich den

SATZ III. *Die Länge des dem Kreisbogen $\widehat{AB}$ eingeschriebenen Linienzuges $AP_1P_2 \cdots P_{n-1}B$ strebt einem bestimmten endlichen Grenzwert zu, falls der größte der Bogen $\widehat{AP_1}, \widehat{P_1P_2}, \ldots, \widehat{P_{n-1}B}$ gegen Null konvergiert.*

Sind nämlich die Sehnen der betreffenden Bogen der Reihe nach $s_1, s_2, \ldots, s_n$ und ist dem Bogen $\widehat{AB}$ entsprechender Zentriwinkel ω, so folgt

1 PAUL SZÁSZ, Neue Herleitung der hyperbolischen Trigonometrie in der Ebene, *Acta Scientiarum Mathematicarum*, **12 A** (1950), S. 44—52, besonders § 1.

2 PAUL SZÁSZ, a. a. O., S. 46, Formel (5).

aus der obigen Formel für $K(r)$ mit einem Schlage

$$s_1+s_2+\cdots+s_n\to\omega K(r)$$

für max $\widehat{P_{i-1}P_i}\to 0\ (P_0=A,\ P_n=B)$.

Einen anderen Beweis, der vom Parallelenaxiom abhängt (aber davon leicht befreit werden kann), hat für diesen Satz III E. EGERVÁRY[3] gegeben.

Nach der üblichen Definition heißt der Grenzwert der Länge des dem Kreisbogen $\widehat{AB}$ eingeschriebenen Linienzuges $AP_1P_2\cdots P_{n-1}B$ für max $\widehat{P_{i-1}P_i}\to 0\ (P_0=A,\ P_n=B)$, die Bogenlänge von $\widehat{AB}$.

Wir heben mit Nachdruck hervor, daß *diese Darstellung der Rektifikation des Kreisbogens vom Parallelenaxiom unabhängig ist und auf Grenzkreisbogen sowie auf Abstandslinienbogen der hyperbolischen Geometrie übertragen werden kann.* Bei dieser Übertragung treten mit geeigneter Modifikation an die Stelle der Maßzahlen der Zentriwinkel die Maßzahlen der Grenzkreis- bzw. Abstandslinienbogen in Bezug auf einen festgehaltenen *Bogen* (der betreffenden Linie) als Einheit. Das hätte schon bei der obigen Darstellung der Kreismessung geschehen können. Unsere Methode hat den Vorteil, daß solcherweise betreffs der Bogenlänge folgender Satz von sich selbst ergibt.

SATZ. *Bedeutet p die Bogenlänge eines Kreis-, Grenzkreis-, oder Abstandslinienbogens $\widehat{AB}$ und s die zugehörige Sehne, so strebt (bei festgehaltenem Radius bzw. Abstand) $\frac{p}{s}\to 1$ für $\widehat{AB}\to 0$.*

In der Tat nimmt bei jeder Kreisart $\frac{p}{s}$ auf Grund des dem Satze I entsprechenden Satzes bei Verkleinerung von p monoton ab, besitzt daher einen gewissen endlichen Grenzwert G für $\widehat{AB}\to 0$, und infolge des den Satz III vertretenden Satzes ist $G=1$, gemäß der Definition der Bogenlänge.

Dieser Satz bildet unserer Meinung nach den einfachsten Grund für die Herleitung der hyperbolischen Trigonometrie mit Hilfe der Grenzkugel.[4] Das erhellt aus den Untersuchungen von M. RÉTHY.[5] Bei dieser Herleitung wird nicht etwa von der Existenz der *Paralleldistanz* Gebrauch gemacht.

(Eingegangen am 10. März 1953.)

[3] E. EGERVÁRY, A remark on the length of the circle and on the exponential function, *Acta Scientiarum Mathematicarum*, **11** (1946), S. 114—118.

[4] Für andere derartige Herleitungen siehe z. B. PAUL SZÁSZ, Neue Herleitung der hyperbolischen Trigonometrie durch Verwendung der Grenzkugel, *Acta Math. Acad. Sci. Hung.*, 3 (1952) S. 327—333, oder Beweis der Hauptformel der hyperbolischen Trigonometrie unabhängig von der Stetigkeit, erscheint demnächst in den *Acta Scientiarum Mathematicarum.*

[5] RÉTHY MÓR, Bolyai János „ujj más világának" ismertetése (ungarisch), *Matematikai és Fizikai Lapok*, 12 (1903), S. 1—29, 303—320, besonders S. 15—18. Vgl. auch PAUL SZÁSZ, a. a. O[1]., § 5., und SZÁSZ PÁL, A hiperbolikus trigonometria közvetlen előállítása a tér felhasználásával (ungarisch), *A Magyar Tudományos Akadémia Matematikai és Fizikai Osztályának Közleményei,* im Erscheinen begriffen.

О СПРЯМЛЕНИИ ОКРУЖНОСТИ, ОРИЦИКЛА И ЭКВИДИСТАНТЫ

П. САС (Будапешт)

(Резюме)

С помощью элементарных рассуждений относительно спрямления кривых постоянной кривизны получается (без использования тригонометнии) теорема о том, что при стремлении длины дуги к 0 отношение длины дуги к хорде стремится к 1. Исследования М. Рети показывают, что эта теорема дает нам самую простую основу для представления гипѐрболической тригонометрии с помощью орисферы.

ÜBER EINEN SATZ VON P. ERDÖS UND P. TURÁN

Von G. FREUD (Budapest)

(*Vorgelegt von* P. TURÁN)

Es sei $\{P_n(x)\}$ die Folge der zur nichtnegativen Gewichtsfunktion $w(x) \in L$ im Orthogonalitätsintervall $(-1, +1)$ gehörenden normierten orthogonalen Polynome. Der Koeffizient von x^n in $P_n(x)$ sei positiv.[1] Die Wurzeln von $P_n(x)$ bezeichnen wir in aufsteigender Reihenfolge mit $x_{1n}, x_{2n}, \ldots, x_{nn}$. Es sei

$$m \leqq w(x) \leqq M \qquad (a \leqq x \leqq b) \tag{1}$$

für ein inneres Teilintervall (a, b) des Orthogonalitätsintervalls $(-1, +1)$. Ferner seien, für ein festes ε, x_{kn} und $x_{k-1,n}$ zwei benachbarte, in $(a+\varepsilon, b-\varepsilon)$ fallende Wurzeln von $P_n(x)$. Dann erhalten wir nach einem Satze von P. ERDÖS und P. TURÁN:

$$\frac{c_1}{n} \leqq x_{k+1,n} - x_{kn} \leqq \frac{c_2}{n} \qquad (a+\varepsilon \leqq x_{kn} \leqq x_{k+1,n} \leqq b-\varepsilon), \tag{2}$$

wobei c_1, c_2 (und im folgenden $c_3, \ldots$) nur von a, b, ε, m und M abhängen, aber von k und n unabhängig sind (P. ERDÖS und P. TURÁN [2], Satz VIII, S. 538). ERDÖS und TURÁN bemerken, daß unter der stärkeren Voraussetzung

$$\frac{m}{\sqrt{1-x^2}} \leqq w(x) \leqq \frac{M}{\sqrt{1-x^2}} \tag{3}$$

für die Zahlen $\vartheta_{kn} = \arccos x_{kn}$ eine Ungleichung der Form (2) in ganzem Orthogonalitätsintervall besteht.[2] Wir zeigen, daß die Ungleichung (2) allgemeiner auch für die in $(-1, +1)$ fallenden Nullstellen x_{kn} des Polynoms

$$Q_n(x) = P_n(x) + AP_{n-1}(x) + BP_{n-2}(x) \qquad (B \leqq 0)$$

besteht, vorausgesetzt, daß alle Wurzeln von $Q_n(x)$ reell und einfach sind. Diese letzte Bedingung ist sicher erfüllt, falls $B = 0$ besteht (G. SZEGŐ [5], Satz 3.34, S. 45). $Q_n(x)$ hat wenigstens $n-2$ Nullstellen, die in das Orthogonalitätsintervall $(-1, +1)$ fallen, da es zu jedem Polynom höchstens $n-3$-ten Grades orthogonal ist. Die Nullstellen des Polynoms $Q_n(x)$, als Grundpunkte einer mechanischen Quadratur, wurden zuerst von L. FEJÉR [3],

[1] Im folgenden wollen wir die orthogonalen Polynome immer in dieser Weise normieren, auch wenn es nicht ausgesprochen wird.

[2] Die ϑ_{kn}, sowie im folgenden die θ_{kn}, sollen in $[0, \pi]$ liegen.

später von P. ERDŐS und P. TURÁN [1] untersucht. Über einige bemerkenswerte Fälle von Polynomen dieser Art verweisen wir auf das Schlußkapitel dieser Mitteilung. Bei dem Beweis werden einige Eigenschaften der mechanischen Quadratur mit den Wurzeln von (4) als Grundpunkte benützt; die hier mitgeteilten Beweise sind an mehreren Stellen von den entsprechenden Beweisgängen von P. ERDŐS und P. TURÁN auch im Falle $A=B=0$ verschieden.

Wir skizzieren den Grundgedanken unseres Beweises für den Fall $A=B=0$. Nach dem klassischen Separationssatz von TSCHEBYSCHEFF, MARKOFF und STIELTJES gilt

$$\sum_{i=1}^{k-1} \lambda_{in} < \int_a^{x_{kn}} w(x)\,dx < \sum_{i=1}^{k} \lambda_{in},$$

wobei λ_{in} die Cotesschen Zahlen bedeuten; hieraus folgt

$$\int_{x_{kn}}^{x_{k+1,n}} w(x)\,dx < \lambda_{kn} + \lambda_{k+1,n}. \tag{4}$$

Nach einem bemerkenswerten Lemma von P. ERDŐS und P. TURÁN [2] folgt aus der rechten Seite von (1) $\lambda_{kn}=O\left(\frac{1}{n}\right)$ und somit besteht

$$x_{k+1,n}-x_{kn} < \frac{1}{m}\int_{x_{kn}}^{x_{k+1,n}} w(x)\,dx = O\left(\frac{1}{n}\right).$$

Die linksstehende Ungleichung in (2) beweisen wir ebenso, wie es von P. ERDŐS und P. TURÁN für den Fall $A=B=0$ durchgeführt wurde.

Wir zeigen, daß die Ungleichung (4) auch für die Cotesschen Zahlen der mechanischen Quadratur über den Nullstellen von $Q_n(x)$ befriedigt ist. In dieser Weise erhalten wir eine recht gute numerische obere Abschätzung für den Abstand zweier benachbarten Nullstellen. Als Anwendung unserer Sätze werden Abschätzungen über die Nullstellenverteilung von Orthogonalpolynomen angegeben, deren Gewichtsfunktion Ungleichungen der Form (42), (44) oder (46) genügt.

Wenn wir auf den genaueren Wert der numerischen Schranke verzichten, kann der Beweis der oberen Abschätzung erheblich abgekürzt werden. Für je drei benachbarte Orthogonalpolynome besteht die Formel

$$P_n(x)=(A_n x+B_n)P_{n-1}(x)-C_n P_{n-2}(x)$$

mit $C_n>0$. Wegen $B\leqq 0$ besitzt also $Q_n(x)$ an den Nullstellen von $P_{n-1}(x)$ dasselbe Vorzeichen, wie $P_n(x)$. Nach einem bekannten Satz hat $P_n(x)$ je einen Vorzeichenwechsel zwischen zwei benachbarten Wurzeln von $P_{n-1}(x)$.

Somit fällt wenigstens eine Wurzel von $Q_n(x)$ zwischen je zwei benachbarte Nullstellen von $P_{n-1}(x)$. Also sind die zwei zu $x_{k,n-1}$ nächstliegenden Nullstellen von $Q_n(x)$ voneinander nicht weiter entfernt als

$$x_{k+1,n-1} - x_{k-1,n-1} = O\left(\frac{1}{n}\right).$$

Den Gedanken dieses letzten Beweises verdanke ich meinem Kollegen P. Szüsz.

Hilfssätze

Die Nullstellen von $Q_n(x)$, die voraussetzungsgemäß alle reell und einfach sind, seien

$$\xi_{1n} < \xi_{2n} < \cdots < \xi_{nn}.$$

Es sei $l_{kn}(x)$ das Lagrangesche interpolatorische Grundpolynom, das zum Grundpunkte ξ_{kn} des Grundpunktsystems $\{\xi_{in}\}$ gehört; also dasjenige Polynom $n-1$-ten Grades, für welches

(5) $$l_{kn}(\xi_{in}) = \delta_{ik} \qquad (i = 1, 2, \ldots, n)$$

besteht. Die Cotesschen Zahlen der mit der Gewichtsfunktion $w(x)$ belegten mechanischen Quadratur mit den Grundpunkten $\{\xi_{in}\}$ seien

(6) $$\lambda_{kn} = \int_{-1}^{+1} l_{kn}(x)\, w(x)\, dx.$$

Hilfssatz I. *Ist $\pi_{2n-3}(x)$ ein beliebiges Polynom höchstens $2n-3$-ten Grades, dann besteht*

(7) $$\int_{-1}^{+1} \pi_{2n-3}(x)\, w(x)\, dx = \sum_{k=1}^{n} \lambda_{kn}\, \pi_{2n-3}(\xi_{kn}).$$

Der Beweis dieses Hilfssatzes beruht auf einem berühmten Gedanken von C. G. J. Jacobi. Es sei

(8) $$\varrho_{n-1}(x) = \sum_{k=1}^{n} \pi_{2n-3}(\xi_{kn})\, l_{kn}(x)$$

das Polynom höchstens $n-1$-ten Grades, das an den Stellen $\{\xi_{kn}\}$ dieselben Werte annimmt, wie $\pi_{2n-3}(x)$. Dann gilt offenbar

(9) $$\pi_{2n-3}(x) - \varrho_{n-1}(x) = [P_n(x) + A\,P_{n-1}(x) + B\,P_{n-2}(x)]\, \pi^*_{n-3}(x),$$

wo $\pi^*_{n-3}(x)$ ein Polynom höchstens $n-3$-ten Grades ist. Aus (9) erhalten wir infolge der Orthogonalität der Polynome $\{P_n(x)\}$

(10) $$\int_{-1}^{+1} [\pi_{2n-3}(x) - \varrho_{n-1}(x)]\, w(x)\, dx = 0,$$

und somit wegen (10), (8) und (6)

$$\int_{-1}^{+1} \pi_{2n-3}(x)\, w(x)\, dx = \int_{-1}^{+1} \varrho_{n-1}(x)\, w(x)\, dx =$$
$$\tag{11} = \sum_{k=1}^{n} \pi_{2n-3}(\xi_{kn}) \int_{-1}^{+1} l_{kn}(x)\, w(x)\, dx = \sum_{k=1}^{n} \lambda_{kn}\, \pi_{2n-3}(\xi_{kn}).$$

HILFSSATZ II. *Sind alle Zahlen* ξ_{kn} $(k = 1, 2, \ldots, n)$ *reell und voneinander verschieden, so gilt*

$$\tag{12} \lambda_{kn} \geqq \int_{-1}^{+1} [l_{kn}(x)]^2 w(x)\, dx > 0 \qquad (k = 1, 2, \ldots, n).$$

Dieser Hilfssatz rührt von L. FEJÉR [3] her (vgl. auch P. ERDŐS und P. TURÁN [1], Gleichung (16c), S. 149). Man beweist ihn ebenso, wie im folgenden die Ungleichung (16).

HILFSSATZ III. ξ_{kn} *und* $\xi_{k+1,n}$ *seien zwei benachbarte, in das Orthogonalitätsintervall* $(-1, +1)$ *fallende Nullstellen von* $Q_n(x)$. *Dann gilt*

$$\tag{13} \int_{\xi_{kn}}^{\xi_{k+1,n}} w(x)\, dx < \lambda_{kn} + \lambda_{k+1,n}.$$

BEWEIS. Nach einem Lemma von P. ERDŐS und P. TURÁN ([2], Lemma IV, S. 529) gilt

$$\tag{14} l_{kn}(x) + l_{k+1,n}(x) \geqq 1 \quad \text{für} \quad \xi_{kn} \leqq x \leqq \xi_{k+1,n}.$$

Zum Beweise muß man berücksichtigen, daß sämtliche ξ_{in} reell sind. Jetzt wollen wir eine veränderte Form des Fejérschen Beweises von Hilfssatz II anwenden: Das Polynom

$$\{l_{kn}(x) + l_{k+1,n}(x)\}^2 - l_{kn}(x) - l_{k+1,n}(x)$$

ist höchstens vom $2n-2$-ten Grade und verschwindet an allen Grundpunkten ξ_{in} $(i = 1, 2, \ldots, n)$. Somit ist es durch $Q_n(x) = P_n(x) + AP_{n-1}(x) + BP_{n-2}(x)$ teilbar:

$$\tag{15} \begin{aligned} &\{l_{kn}(x) + l_{k+1,n}(x)\}^2 - l_{kn}(x) - l_{k+1,n}(x) = \\ &= [P_n(x) + AP_{n-1}(x) + BP_{n-2}(x)]\,[\alpha_{n-2}P_{n-2}(x) + \pi_{n-3}(x)]. \end{aligned}$$

Hierbei ist $\pi_{n-3}(x)$ ein Polynom höchstens $n-3$-ten Grades, also es ist auf $P_n(x)$, $P_{n-1}(x)$ und $P_{n-2}(x)$ orthogonal. Nach Vergleich der Koeffizienten von x^{2n-2} an beiden Seiten von (15) und mit Rücksicht darauf, daß der höchste Koeffizient sowohl in $P_n(x)$, als auch in $P_{n-2}(x)$ positiv ist und an der linken Seite der Koeffizient von x^{2n-2} infolge des Quadrierens positiv ist, erhalten wir, daß $\alpha_{n-2} > 0$, und somit $B\alpha_{n-2}^{*} \leqq 0$ besteht.

Infolge dessen erhalten wir aus (15)

$$\int_{-1}^{+1} \{l_{kn}(x)+l_{k+1,n}(x)\}^2 w(x)\,dx = \tag{16}$$

$$= \int_{-1}^{+1} \{l_{kn}(x)+l_{k+1,n}(x)\}\, w(x)\,dx + B\alpha_{n-2}\int_{-1}^{+1} [P_{n-2}(x)]^2 w(x)\,dx \leqq \lambda_{kn}+\lambda_{k+1,n}.$$

Aus (14) und (16) folgt endlich

$$\int_{\xi_{kn}}^{\xi_{k+1,n}} w(x)\,dx < \int_{-1}^{+1} \{l_{kn}(x)+l_{k+1,n}(x)\}^2 w(x)\,dx \leqq \lambda_{kn}+\lambda_{k+1,n},$$

w. z. b. w.

HILFSSATZ IV a. *Es sei* $w(x) \leqq M$ *in einem inneren Teilintervall* (a, b) *von* $(-1, +1)$. *Falls* ξ_{kn} *in ein festes inneres Teilintervall* $(a+\varepsilon, b-\varepsilon)$ *von* (a, b) *fällt, so besteht*

$$\lambda_{kn} \leqq \frac{c_3}{n}. \tag{17}$$

Für den speziellen Fall $A=B=0$ wurde dieser Hilfssatz von P. ERDÖS und P. TURÁN ([2], Lemma V, S. 530) bewiesen. Die Verallgemeinerung bietet keine neuen Schwierigkeiten: Man konstruiert ein Polynom $\varphi_{n-2}(x)$ vom $n-2$-ten Grade, das den Bedingungen

$$\varphi_{n-2}(\xi_{kn}) = 1, \tag{18}$$

$$\int_{-1}^{+1} [\varphi_{n-2}(x)]^2\,dx < \frac{c_4}{n} \tag{19}$$

und

$$|\varphi_{n-2}(x)| < \frac{c_5}{n} \quad \text{für} \quad |x-\xi_{kn}| > \varepsilon \text{ und } -1 \leqq x \leqq +1 \tag{20}$$

genügt. Nach Hilfssatz I gilt wegen (12), (19) und (20)

$$\lambda_{kn} < \sum_{i=1}^{n} \lambda_{in}[\varphi_{n-2}(\xi_{in})]^2 = \int_{-1}^{+1} [\varphi_{n-2}(x)]^2 w(x)\,dx <$$

$$< M\int_{-1}^{+1} [\varphi_{n-2}(x)]^2\,dx + \frac{c_5^2}{n^2}\int_{-1}^{+1} w(x)\,dx < \frac{c_3}{n},$$

w. z. b. w.

HILFSSATZ IV b. *Es sei* $w(x) \leqq M(1-x^2)^{-1/2}$ *im ganzen Orthogonalitätsintervall* $(-1, +1)$. *Dann besteht für jede Cotessche Zahl* λ_{kn}, *deren Grund-*

punkt ξ_{kn} *in* $(-1, +1)$ *fällt*

$$\lambda_{kn} \leqq \frac{2\pi M}{2n-3-\dfrac{1}{\sin\dfrac{\pi}{2n-3}}} \quad \text{für} \quad n>2. \tag{21}$$

Ist ferner $\xi_{kn} = \cos\theta_{kn}$ *und* $\frac{\pi}{2}-\alpha \leqq \theta_{kn} \leqq \frac{\pi}{2}+\alpha$ $\left(\alpha < \frac{\pi}{2}\right)$, *dann gilt sogar*

$$\lambda_{kn} \leqq \frac{2\pi M}{2n-3-\cos^{-1}\alpha}. \tag{22}$$

BEWEIS. Durchläuft $\pi_{n-2}(x)$ alle Polynome höchstens vom $n-2$-ten Grade mit $\pi_{n-2}(\xi_{kn})=1$, dann gilt infolge eines Lemmas von P. ERDŐS und P. TURÁN ([2], S. 539):

$$\operatorname*{Min}_{\pi_{n-2}(\xi_{kn})=1} \int_{-1}^{+1} \frac{[\pi_{n-2}(x)]^2}{\sqrt{1-x^2}}\,dx = \frac{2\pi}{2n-3+\dfrac{\sin(2n-3)\theta_{kn}}{\sin\theta_{kn}}} \tag{23}$$

und dieses Minimum wird bei geeigneter Wahl von $\pi_{n-2}(x)$ tatsächlich angenommen; im folgenden sei $\pi_{n-2}(x)$ eben dieses Polynom, das in (23) das Minimum liefert. Aus (7), (12) und (23) erhalten wir

$$\begin{aligned} \lambda_{kn} &\leqq \sum_{i=1}^{n} \lambda_{in}[\pi_{n-2}(\xi_{in})]^2 = \int_{-1}^{+1} [\pi_{n-2}(x)]^2 w(x)\,dx \leqq \\ &\leqq M \int_{-1}^{+1} \frac{[\pi_{n-2}(x)]^2}{\sqrt{1-x^2}}\,dx = \frac{2\pi M}{2n-3+\dfrac{\sin(2n-3)\theta_{kn}}{\sin\theta_{kn}}}. \end{aligned} \tag{24}$$

Hieraus folgt (22) unmittelbar. Um (21) zu beweisen, genügt es zu zeigen, daß

$$\frac{\sin(2n-3)\varphi}{\sin\varphi} \geqq -\frac{1}{\sin\dfrac{\pi}{2n-3}}. \tag{24}$$

Für $0 \leqq \varphi \leqq \frac{\pi}{2n-3}$ ist diese Ungleichung trivial, da die linke Seite positiv ist; ist dagegen $\frac{\pi}{2n-3} \leqq \varphi \leqq \frac{\pi}{2}$, so besteht (25) wegen $|\sin(2n-3)\varphi| \leqq 1$ und $\sin\varphi > \sin\frac{\pi}{2n-3}$. Endlich nimmt die linke Seite von (25) für φ und $\pi-\varphi$ dieselben Werte an, womit unser Beweis beendet ist. (Es sei bemerkt, daß in (22) die Zahl 2π durch keine kleinere ersetzt werden kann.)

Abschätzung des Abstandes benachbarter Nullstellen

SATZ I a. *Die Gewichtsfunktion $w(x)$ befriedige in einem inneren Teilintervall (a, b) von $(-1, +1)$ die Ungleichung* (1). *Fallen ξ_{kn} und $\xi_{k+1,n}$ in ein inneres Teilintervall $(a+\varepsilon, b-\varepsilon)$ von (a, b), dann besteht die Ungleichung*

$$\xi_{k+1,n}-\xi_{kn} \leqq \frac{c_6}{n}. \tag{26}$$

BEWEIS. Aus (1), (13) und (17) folgt

$$\xi_{k+1,n}-\xi_{kn} \leqq \frac{1}{m}\int_{\xi_{kn}}^{\xi_{k+1,n}} w(x)\,dx < \frac{1}{m}(\lambda_{kn}+\lambda_{k+1,n}) \leqq \frac{2c_8}{m}\frac{1}{n},$$

w. z. b. w.

SATZ I b. *Es genüge $w(x)$ im ganzen Orthogonalitätsinterwall $(-1, +1)$ der Ungleichung* (3). *Sind $\xi_{kn}=\cos\theta_{kn}$ und $\xi_{k+1,n}=\cos\theta_{k+1,n}$ zwei benachbarte, in $(-1, +1)$ fallende Wurzeln von $Q_n(x)$, dann gilt für $n>2$*

$$\theta_{kn}-\theta_{k+1,n} \leqq \frac{M}{m}\,\frac{4\pi}{2n-3-\dfrac{1}{\sin\dfrac{\pi}{2n-3}}}. \tag{27}$$

Ist ferner $\frac{\pi}{2}-\alpha<\theta_{k+1,n}<\theta_{kn}<\frac{\pi}{2}+\alpha$ mit $\alpha<\frac{\pi}{2}$, so besteht die Ungleichung

$$\theta_{kn}-\theta_{k+1,n} \leqq \frac{M}{m}\,\frac{4\pi}{2n-3-\cos^{-1}\alpha}. \tag{28}$$

BEWEIS. Wegen (3) und (13) gilt

$$\theta_{kn}-\theta_{k+1,n} = \int_{\xi_{kn}}^{\xi_{k+1,n}} \frac{dx}{\sqrt{1-x^2}} \leqq \frac{1}{m}\int_{\xi_{kn}}^{\xi_{k+1,n}} w(x)\,dx \leqq \frac{1}{m}(\lambda_{kn}+\lambda_{k+1,n}) \tag{29}$$

und hieraus folgt (27), bzw. (28) aus (21) und (29), bzw. (22) und (29). (Die Zahl 4π in (28) kann gewiß nicht durch eine Zahl kleiner als 2π ersetzt werden.)

SATZ II a. *Es genüge $w(x)$ der Ungleichung* (1). *Dann gilt für zwei benachbarte Nullstellen ξ_{kn} und $\xi_{k+1,n}$, die in ein festes inneres Teilintervall $(a+\varepsilon, b-\varepsilon)$ von (a, b) fallen, die Ungleichung*

$$\xi_{k+1,n}-\xi_{kn} \geqq \frac{c_7}{n}. \tag{30}$$

BEWEIS. Infolge (12) und (17) gilt

$$\int_a^b [l_{nk}(x)]^2\,dx < \frac{1}{m}\int_{-1}^{+1} [l_{kn}(x)]^2 w(x)\,dx < \frac{1}{m}\lambda_{kn} < \frac{c_8}{n}. \tag{31}$$

Im weiteren wird derselbe Beweisgang verfolgt, wie in der Arbeit [2] von P. ERDŐS und P. TURÁN. Wegen (31) besteht

$$0<\int_a^x [l_{kn}(t)]^2\,dt<\frac{c_8}{n},$$

woraus mittels zweimaliger Anwendung des Polynomensatzes von BERNSTEIN

$$\left|\frac{d}{dx}[l_{nk}(x)]^2\right|\leqq c_9 n \quad \text{für} \quad a+\varepsilon\leqq x\leqq b-\varepsilon \tag{32}$$

folgt. Beachten wir, daß $l_{kn}(\xi_{kn})=1$ und $l_{kn}(\xi_{k+1,n})=0$ ist; dann erhalten wir unter Anwendung des Lagrangeschen Mittelwertsatzes der Differentialrechnung

$$1=[l_{kn}(\xi_{kn})]^2-[l_{kn}(\xi_{k+1,n})]^2\leqq(\xi_{k+1\,n}-\xi_{kn})\max_{\xi_{kn}\leqq\xi\leqq\xi_{k+1,n}}\left|\frac{d}{d\xi}[l_{kn}(\xi)]^2\right|. \tag{33}$$

Aus (32) und (33) folgt (30), w. z. b. w.

SATZ II b. *Es befriedige* $w(x)$ *die Ungleichung* (3). *Sind* $\xi_{kn}=\cos\theta_{kn}$ *und* $\zeta_{k+1,n}=\cos\theta_{k+1,n}$ *zwei benachbarte, in* $(-1,+1)$ *fallende Wurzeln von* $Q_n(x)$, *dann besteht die Ungleichung*

$$\theta_{kn}-\theta_{k+1,n}\geqq\frac{1}{40}\frac{m}{M}\cdot\frac{1}{n}. \tag{34}$$

BEWEIS. Beachten wir, daß

$$\lambda_{kn}=\int_0^\pi [l_{kn}(\cos\theta)]^2 w(\cos\theta)\sin\theta\,d\theta$$

gilt, ferner infolge (3)

$$m\leqq w(\cos\theta)\sin\theta\leqq M$$

erfüllt ist, so erhalten wir

$$\frac{1}{M}\lambda_{kn}\leqq\int_0^\pi[l_{kn}(\cos\theta)]^2\,d\theta=\Lambda_{kn}\leqq\frac{1}{m}\lambda_{kn},$$

und hieraus folgt

$$-\frac{1}{m}\lambda_{kn}\leqq-\frac{1}{\pi m}\lambda_{kn}+\frac{1}{M}\lambda_{kn}\leqq\int_0^\theta\left\{[l_{kn}(\cos\theta)]^2-\frac{1}{\pi}\Lambda_{kn}\right\}d\theta=F(\theta)\leqq\frac{1}{m}\lambda_{kn}.$$

Beachten wir ferner, daß $F(\theta)$ ein trigonometrisches Polynom ist, dessen Grad $2n$ nicht überschreitet, so erhalten wir infolge (21) mittels zweimaliger Anwendung des Satzes von BERNSTEIN:

$$\left|\frac{d}{d\theta}[l_{kn}(\cos\theta)]^2\right|\leqq\frac{(2n)^2}{m}\lambda_{kn}\leqq\frac{4n^2}{m}\,\frac{2\pi M}{2n-3-\dfrac{1}{\sin\dfrac{\pi}{2n-3}}}<40\frac{M}{m}n. \tag{35}$$

Der letzte Schritt ist derselbe, wie in (33).

SATZ III. *Es genüge* $w(x)$ *der Ungleichung* (3); $\xi^* = \cos\theta^*$ *bzw.* $\xi^{**} = \cos\theta^{**}$ *seien die größte, bzw. die kleinste* $(-1, +1)$ *fallende Nullstelle von* $Q_n(x)$ $(n > 2)$; *dann gilt*

$$(36)\qquad \theta^* \leqq \frac{M}{m}\,\frac{4\pi}{2n-3-\dfrac{1}{\sin\dfrac{\pi}{2n-2}}} \quad \textit{und} \quad \pi-\theta^{**} \leqq \frac{M}{m}\,\frac{4\pi}{2n-3-\dfrac{1}{\sin\dfrac{\pi}{2n-3}}}.$$

BEWEIS. Offenbar genügt es, die erste der beiden Ungleichungen zu beweisen. Zuerst betrachten wir den Fall, daß $Q_n(x)$ außerhalb des offenen Intervalles $(-1, +1)$ keine solche Nullstelle besitzt, die größer als ξ^* ist, d. h. $\xi^* = \xi_{nn}$. Betrachten wir das Grundpolynom $l_{nn}(x)$. Das ist ein Polynom $n-1$-ten Grades, welches $n-1$ links von ξ_{nn} fallende Nullstellen besitzt. Infolge dessen hat $\dfrac{dl_{nn}(x)}{dx}$ je einen Zeichenwechsel in den Intervallen

$$(\xi_{1n}, \xi_{2n}), (\xi_{2n}, \xi_{3n}), \ldots, (\xi_{n-2,n}, \xi_{n-1,n})$$

und weitere Zeichenwechsel kann es nicht haben. Wegen $l_{nn}(\xi_{n-1,n}) = 0$ und $l_{nn}(\xi_{nn}) = 1$ ist $l_{nn}(x)$ für $x > \xi_{n-1,n}$ monoton wachsend, also gilt

$$(37)\qquad l_{nn}(x) \geqq 1 \quad \text{für} \quad x \geqq \xi_{nn}.$$

Deshalb ergibt sich aus (3), (12) und (21)

$$(38)\qquad \theta^* = \theta_{nn} < \frac{1}{m}\int_0^{\theta_{nn}} [l_{nn}(\cos\theta)]^2 w(\cos\theta)\sin\theta\, d\theta <$$

$$< \frac{1}{m}\int_0^{\pi} [l_{nn}(\cos\theta)]^2\, w(\cos\theta)\,.\,\sin\theta\, d\theta \leqq \frac{1}{m}\lambda_{nn} \leqq \frac{M}{m}\,\frac{2\pi}{2n-3-\dfrac{1}{\sin\dfrac{\pi}{2n-3}}}.$$

Zweitens betrachten wir den Fall, daß $Q_n(x)$ eine Nullstelle $> \xi^*$ besitzt; die kleinste Nullstelle dieser Art sei ξ^{**}. Die Lagrangesche interpolatorische Grundfunktion, die zum Grundpunkte ξ^* bzw. ξ^{**} gehört, sei $l_n^*(x)$ bzw. $l_n^{**}(x)$; die entsprechenden Cotesschen Zahlen seien λ_n^* bzw. λ_n^{**}. Wegen (14) und (16) folgt aus (21)

$$\theta^* \leqq \frac{1}{m}\int_0^{\theta^*} [l_n^*(\cos\theta) + l_n^{**}(\cos\theta)]^2 w(\cos\theta)\sin\theta\, d\theta \leqq$$

$$(39)\qquad \leqq \frac{1}{m}\int_{-1}^{+1} [l_n^*(x) + l_n^{**}(x)]^2 w(x)\, dx \leqq \frac{1}{m}(\lambda_n^* + \lambda_n^{**}) \leqq$$

$$\leqq \frac{M}{m}\,\frac{2\pi}{2n-3-\dfrac{1}{\sin\dfrac{\pi}{2n-3}}} + \frac{1}{m}\lambda_n^{**}.$$

Es bleibt noch die Abschätzung von λ_n^{**} übrig. Betrachten wir das Polynom $\psi_{n-2}(x)=\frac{1}{n-1}U_{n-2}(x)$, wobei $U_{n-2}(x)$ das $n-2$-te Tschebyscheffsche Polynom zweiter Art bedeutet. Wegen $\psi_{n-2}(1)=1$ und $\xi^{**}\geqq 1$ gilt

$$\psi_{n-2}(\xi^{**})\geqq 1. \tag{40}$$

Somit erhalten wir aus (12) infolge $w(x)\leqq M(1-x^2)^{-1/2}$

$$\begin{aligned}\lambda_n^{**}&\leqq\sum_{k=1}^{n}\lambda_{kn}[\psi_{n-2}(\xi_{kn})]^2=\int_{-1}^{+1}[\psi_{n-2}(x)]^2w(x)\,dx\leqq\\&\leqq\frac{M}{(n-1)^2}\int_{-1}^{+1}[U_{n-2}(x)]^2\frac{dx}{\sqrt{1-x^2}}\leqq\frac{M\pi}{n-1}.\end{aligned}\tag{41}$$

Infolge (38), bzw. (39) und (41) ist (36) erfüllt, w. z. b. w.

Anwendungen

SATZ IV. *Es bezeichne $p_n(x)$ das Polynom n-ten Grades des orthogonalen Polynomsystems, welches zu der der Forderung*

$$m\sqrt{1-x^2}\leqq w(x)\leqq M\sqrt{1-x^2} \tag{42}$$

genügenden Gewichtsfunktion $w(x)$ gehört. Sind $x_{1n}<x_{2n}<\cdots<x_{nn}$ die Nullstellen von $p_n(x)$, ferner $x_{0n}=-1$, $x_{n+1,n}=+1$, dann besteht mit der Bezeichnung $x_{kn}=\cos\theta_{kn}$ die Ungleichung

$$\frac{1}{40}\frac{m}{M}\frac{1}{n+2}\leqq\theta_{kn}-\theta_{k+1,n}\leqq\frac{M}{m}\frac{4\pi}{2n+1-\dfrac{1}{\sin\dfrac{\pi}{2n+1}}}\qquad(k=0,1,\ldots,n). \tag{43}$$

Ist ferner $\frac{\pi}{2}-\alpha<\theta_{k+1,n}<\theta_{kn}<\frac{\pi}{2}+\alpha$ mit $\alpha<\frac{\pi}{2}$, dann ist auch (28) *erfüllt.*

BEWEIS. Es sei $\{P_n(x)\}$ die Folge der zur Gewichtsfunktion $w^*(x)=(1-x^2)^{-1}w(x)$ gehörenden orthogonalen Polynome. Wir entwickeln $(x^2-1)p_n(x)$ nach dem Orthogonalsystem $\{P_n(x)\}$:

$$(x^2-1)p_n(x)=\sum_{k=0}^{n+2}c_kP_k(x)$$

mit

$$c_k=\int_{-1}^{+1}(x^2-1)p_n(x)P_k(x)w^*(x)\,dx=-\int_{-1}^{+1}p_n(x)P_k(x)w(x)\,dx.$$

Hieraus ersieht man sofort, daß $c_k=0$ für $k<n$. Außerdem erhalten wir, wenn wir mit $\varkappa_n$ den Koeffizienten von x^n in $p_n(x)$ und mit k_n den Koeffi-

zienten von x^n in $P_n(x)$ bezeichnen, durch Koeffizientenvergleich

$$c_{n+2} = \frac{\varkappa_n}{k_{n+2}} > 0.$$

Endlich ergibt sich

$$c_n = -\int_{-1}^{+1} p_n(x) P_n(x) w(x)\, dx = -\int_{1}^{+1} p_n(x) \left[\frac{k_n}{\varkappa_n} p_n(x) + \cdots\right] w(x)\, dx =$$
$$= -\frac{k_n}{\varkappa_n} < 0.$$

Aus diesen Überlegungen folgt

$$(x^2-1) p_n(x) = \frac{\varkappa_n}{k_{n+2}} [P_{n+2}(x) + A P_{n+1}(x) + B P_n(x)] \quad \text{mit} \quad B < 0.$$

Da die Gewichtsfunktion $w^*(x) = (1-x^2)^{-1} w(x)$ infolge (42) die Ungleichung (3) befriedigt, folgt Satz IV aus den Sätzen I b und II b, w. z. b. w.

SATZ V. *Es bezeichne $p_n(x)$ das orthogonale Polynom n-ten Grades, welches zur Gewichtsfunktion $w(x)$ gehört, die der Forderung*

$$m\sqrt{\frac{1-x}{1+x}} \leqq w(x) \leqq M\sqrt{\frac{1-x}{1+x}} \tag{44}$$

genügt. Die Nullstellen von $p_n(x)$ seien in aufsteigender Folge $x_{kn} = \cos\theta_{kn}$ $(k = 1, 2, \ldots, n)$ und es sei $x_{n+1,n} = +1$; dann besteht die Ungleichung

$$\frac{1}{40}\frac{m}{M}\frac{1}{n+1} \leqq \theta_{kn} - \theta_{k+1,n} \leqq \frac{M}{m} \frac{4\pi}{2n-1-\dfrac{1}{\sin\dfrac{\pi}{2n-1}}} \qquad (k = 1, 2, \ldots, n). \tag{45}$$

Eine ähnliche Behauptung besteht, falls die Gewichtsfunktion der Ungleichung

$$m\sqrt{\frac{1+x}{1-x}} \not\leqq w(x) \leqq M\sqrt{\frac{1+x}{1-x}} \tag{46}$$

genügt.

BEWEIS. Wir bezeichnen mit $\{P_n(x)\}$ die Folge derjenigen orthogonalen Polynome, die zur Gewichtsfunktion $w^*(x) = (1-x)^{-1} w(x)$ gehören. Mit derselben Schlußweise, wie bei Satz IV, ergibt sich

$$(1-x) p_n(x) = -\frac{\varkappa_n}{k_{n+1}} P_{n+1}(x) + \frac{k_n}{\varkappa_n} P_n(x),$$

und somit ist auch Satz IV auf die Sätze I b und II b zurückgeführt.

(Eingegangen am 8. Juni 1953.)

Literatur

[1] P. Erdős—P. Turán, On interpolation. I, *Annals of Math.*, **38** (1937), S. 142—155.
[2] P. Erdős—P. Turán, On interpolation. III, *Annals of Math.*, **41** (1940), S. 510—553.
[3] L. Fejér, Mechanische Quadraturen mit positiven Cotesschen Zahlen, *Math. Zeitschr.*, **37** (1933), S. 287—310.
[4] C. G. J. Jacobi, Ueber Gauss's neue Methode, die Werthe der Integrale näherungsweise zu finden, *Journal f. reine u. angew. Math.*, **1** (1826), S. 301—308.
[5] G. Szegő, *Orthogonal polynomials*, Amer. Math. Soc. Coll. Publ., Vol. XXIII. (New York, 1939.)

ОБ ОДНОЙ ТЕОРЕМЕ П. ЭРДЁША И П. ТУРАНА

Г. ФРАЙД (Будапешт)

(Резюме)

Рассмотрим семейство $\{P_n(x)\}$ многочленов, ортогональным на отрезке $(-1, +1)$ относительно неотрицательного веса $w(x)$. На внутренней части (a, b) отрезка $(-1, +1)$ пусть имеет место

$$0 < m \leqq w(x) \leqq M,$$

и пусть все корни многочлена

$$Q_n(x) = P_n(x) + AP_{n-1}(x) + BP_{n-2}(x) \qquad (B < 0)$$

вещественны. В этом случае расстояние двух соседних корней многочлена $Q_n(x)$, попадающих в $(a+h, b-h)$, удовлетворяет условию

$$\frac{c_1}{n} \leqq x_{k+1,n} - x_{k,n} \leqq \frac{c_2}{n}.$$

Если же

$$\frac{m}{\sqrt{1-x^2}} \leqq w(x) \leqq \frac{M}{\sqrt{1-x^2}}$$

и $\theta_{k,n} = \arccos x_{k,n}$, то

$$\frac{1}{4D}\,\frac{m}{M}\cdot\frac{1}{n} \leqq \theta_{k,n} - \theta_{k+1,n} \leqq \frac{M}{m}\,\frac{4\pi}{2n-3-\dfrac{1}{\sin\dfrac{\pi}{2n-3}}}$$

и если $\alpha \leqq \theta_{k+1,n} < \theta_{k,n} \leqq \pi - \alpha$, тогда

$$\theta_{k,n} - \theta_{k+1,n} \leqq \frac{M}{m}\,\frac{4\pi}{2n-3-\cos^{-1}\alpha}.$$

Используя эти неравенства выводятся подобные оценки расстояния корней ортогонального многочлена $P_n(x)$ для случая, когда $w(x)$ удовлетворяет одному из неравенств

$$m\sqrt{1-x^2} \leqq w(x) \leqq M\sqrt{1-x^2},$$

$$m\sqrt{\frac{1-x}{1+x}} \leqq w(x) \leqq M\sqrt{\frac{1-x}{1+x}},$$

$$m\sqrt{\frac{1+x}{1-x}} \leqq w(x) \leqq M\sqrt{\frac{1+x}{1-x}}.$$

Верхняя оценка расстояния корней дается на основе следующей вспомогательной теоремы:

Пусть $\lambda_{k,n}$ число Cotes'a, принадлежащее узле $x_{k,n}$ системы узлов $(x_{1n}, x_{2n}, \ldots, x_{nn})$ при весе $w(x)$. Тогда

$$\int_{x_{k,n}}^{x_{k+1,n}} w(x)\,dx < x_{k,n} + \lambda_{k+1,n}.$$

ON THE STRUCTURE OF ABELIAN p-GROUPS

By

L. FUCHS (Budapest)

(*Presented by* L. RÉDEI)

§ 1. Introduction

The classical basis theorem for finite abelian groups[1] has been generalized in a number of different directions, for example, to finitely generated abelian groups, to such groups with a Euclidean operator ring, to groups of finite rank[2] etc. All of these theorems describe the groups under consideration by a finite set of invariants, by giving a direct decomposition into groups (uniquely determined up to isomorphisms) whose structures are very simple and are completely known. However, such direct decompositions fail to exist in general. The recognition of this fact has given rise to several attempts of getting structure theorems, not necessarily in terms of direct decompositions, for a rather wide class of groups. In order to give a survey of a part of these results, let us first observe that the basis theorem for finite abelian groups may be regarded to consist of the following three assertions:

1) *unique decomposition*, i. e. representability as the direct sum of cyclic groups of uniquely determined prime-power orders;

2) *isomorphism statement:* two groups having the same direct decomposition are isomorphic;

3) *existence statement:* if given a finite set of cyclic groups, then there is a finite group isomorphic to their direct sum.

Among the infinite groups there are two important classes for which the analogues of 1)—3) are well known: the torsion free groups of finite rank and the countable p-groups (and hence all countable torsion groups). For the former class the analogues of 1)—3) are due to A. KUROSH, A. MALCEV and D. DERRY,[3] while for the latter class to H. PRÜFER, H. ULM and L. ZIPPIN.[4]

[1] For brevity, in the sequel we say simply group instead of abelian group.

[2] See e. g. KUROSH [10] or SZELE [17], Satz 11. By the *rank* of a group G we mean the cardinal number of a maximal independent system of elements in G containing but elements of infinite or prime-power order; see § 2.

[3] See KUROSH [11] and [12], MALCEV [14] and DERRY [2].

[4] See PRÜFER [15], ULM [19] and ZIPPIN [21].

As we shall be concerned here with p-groups, let us consider in detail the analogues of 1)—3) for countable p-groups.[5]

1′) With each p-group G one can associate the so-called Ulm sequence

$$G_0, G_1, \ldots, G_\alpha, \ldots$$

which is a well-ordered set of p-groups $G_\alpha (\neq 0)$ uniquely determined by G. If G is reduced — and only such groups must be discussed — then its Ulm sequence terminates with an ordinal τ which is finite or countable if G is countable. Since no G_α contains elements of infinite height, and $|G| = \aleph_0$ implies $|G_\alpha| = \aleph_0$,[6] by PRÜFER's well-known theorem one obtains that each G_α is the direct sum of cyclic p-groups whose orders are uniquely determined by G.

2′) The isomorphism statement has also an analogue in the form of a theorem of ULM. This states that if two countable p-groups have the same Ulm sequence, then they are necessarily isomorphic. 1′) and 2′) show that the groups in question may uniquely be characterized by invariants, though in a manner not so simple as in the finite case.

3′) The existence theorem is due to ZIPPIN. He has proved that to any well-ordered (countable) sequence of unbounded[7] countable p-groups $G_\alpha (\alpha < \tau)$ without elements of infinite height there exists a reduced p-group having the given sequence for its Ulm sequence.

These fundamental theorems completely settle the structure problem for countable p-groups. However, the methods used for countable groups have proved to be unapplicable to groups of power $> \aleph_0$. Several examples[8] have been given to show that PRÜFER's theorem ceases to hold for groups of power $\geqq \aleph$, moreover, as it was recently shown by T. SZELE,[9] for groups of power $\aleph_1$. The problem of abelian p-groups beyond the countable ones seemed to be hopelessly far from solution until the publication of a paper by L. KULIKOV [8], surmounting a good deal of difficulties arising in the case of arbitrary power. In this paper has KULIKOV introduced the important concept of basic subgroup, a concept which is, in the author's opinion, the most fundamental tool in the theory of abelian p-groups of power $> \aleph_0$. In the same paper KULIKOV has shown that the analogue of ULM's theorem does not hold in general, moreover, two groups with the same Ulm sequence need not be even of the same power. The question as to whether or not ZIPPIN's theorem may be extended in a suitable manner to groups of arbitrary power has been settled recently by KULIKOV [9] in a generalized form (namely, instead for p-groups

[5] For the terminology and notation see § 2.

[6] $G_{\tau-1}$, if exists, may be finite, but in all other Ulm factors the orders of the elements have no upper bound (such groups will be called *unbounded* groups).

[7] $G_{\tau-1}$ need not be unbounded, cf. [6].

[8] See e. g. ULM [20] or KUROSH [12].

[9] SZELE [18].

also for generalized p-groups, i. e. for groups having certain operator ring). Not knowing of his result, I have also solved this problem[10] by giving necessary and sufficient conditions for the Ulm sequence which ensure the existence of a reduced p-group G of a prescribed power $\mathfrak{p}$ and type τ, and with the given Ulm sequence G_α. The concluding part of KULIKOV's proof is not yet appeared, but from the introduction of his paper [9] it turns out undoubtedly that the most essential idea of my proof has not been used by KULIKOV. Besides, although the solution of this problem is considered by KULIKOV himself as the principal result of his paper [9], there are several other very important results and significant methods contained in the paper which do not lie closely on the way leading to the generalized Zippin theorem. Therefore, perhaps it would not be quite superfluous if I publish here my original proof for readers interested merely in the analogue of ZIPPIN's theorem for p-groups (leaving the case of generalized primary groups out of consideration).

After laying down the terminology and notation we shall need, we turn our attention to the basic subgroup. Among others we show that each basic subgroup gives rise to a generating system of the whole group by which each element in the group may be expressed in a unique manner so that it may be considered as a substitute for the basis, in the general case. This is the reason why we shall call it a quasibasis.

In the next section we prove a theorem which is, in a certain sense, an analogue of PRÜFER's theorem mentioned above, in the general case. Since direct decompositions in general fail to exist, one may suggest that perhaps a similar decomposition exists if one admits, instead of direct sum, some suitable generalization of the notion of direct sum. Indeed, the concept of interdirect sum due to T. SZELE[11] is an adequate notion for this purpose. By making use of this concept, we can prove, for p-groups containing no elements of infinite height, the existence of a representation as an interdirect sum of cyclic groups. This theorem is equivalent to a result of KULIKOV,[12] but will be proved here directly, without appeal to [8]. The interdirect sum is a subdirect sum containing each component, so that this structure theorem is a deeper result, tells us much more about the group structure than the usual structure theorems in terms of subdirect sums in ring theory. However, the structure theorems in terms of interdirect sums can not be regarded as satisfactory as those in terms of direct sums, for, if given an infinite set of groups, then there is a great variety of their interdirect sums.

Our discussion of the generalization of ZIPPIN's theorem rests on two main observations. The first of these is that the power of an Ulm factor G_α

10 My results were first published in a lecture held before the J. Bolyai Mathematical Society, 14 February 1953.

11 Cf. KERTÉSZ and SZELE [6] as well as SZELE and SZENDREI [16].

12 KULIKOV [8], § 5 or KUROSH [13], p. 168.

must have some effect on the totality of the powers of the following Ulm factors. In this connection a remarkable fact is that already the first ω Ulm factors give an upper bound for the power of the group. The second, and more essential, observation is that all elements of an Ulm factor G_α become of infinite height if the generating elements of a basic subgroup B_α of G_α are of infinite height. This fact makes essentially simpler the proof, for we have only to take care of the basis of B_α, and not of all elements of G_α. In view of the first observation it seems natural to perform the demonstration in two steps, at first for groups of type $\leqq \omega$ and then for the general case. The result enables us to give examples showing that ULM's theorem can not be generalized to groups of power $> \aleph_0$

Consequently, we have the following analogues of 1)—3) in case of groups of arbitrary power:

1″) Each p-group has an Ulm sequence G_α consisting of groups representable as a (restricted and serving) interdirect sum of cyclic groups whose orders are uniquely determined (§ 4).

2″) ULM's theorem does not hold for groups of power $\geqq \aleph_1$ (§ 8).

3″) There are necessary and sufficient conditions which guarantee the existence of a reduced p-group if its power, its type and its Ulm sequence are given (§§ 5, 7).

§ 2. Notation and terminology

By a group we shall mean an additively written abelian p-group with more than one element. The prime p is arbitrary, but is fixed throughout the discussion. Cyclic groups of order p^n will be denoted by $\mathfrak{Z}(p^n)$, while $\mathfrak{Z}(p^\infty)$ will denote the *quasicyclic* group, i. e. the group of type p^∞ introduced by PRÜFER. It is known that an *algebraically closed*[13] (i. e. a *complete*) p-group G (defined so as to satisfy $nG = G$ for all non-zero integers n) is the direct sum of quasicyclic groups and is a direct summand of every containing (abelian) group.[14] If G is some group then the union A of all algebraically closed subgroups of G is again algebraically closed and so we have $G = A + G'$ where G' is *reduced*, i. e. it contains no algebraically closed subgroup other than 0. Since the structure of G is completely known if G' is known, one may without loss of generality confine himself to the discussion of reduced groups.

The following notation will be used. We denote by $O(x)$ the order of the group element x and by $\{S\}$ the subgroup generated by a subset S of G. $|G|$ will mean the power of G.

[13] See e. g. SZELE [17].

[14] See BAER [1].

For an element a the maximal non-negative integer h for which the equation $p^h x = a$ has a solution in G is said to be the *height* of a, in notation: $H(a) = h$. In case there is no greatest h of this property, then we say a is of infinite height. For the sake of convenience, we agree to consider the zero element to be both of infinite height and not.[15] A subgroup H of G is termed a *serving* subgroup of G if for each $a \in H$ the solvability of $nx = a$ in G implies its solvability in H, i. e. the elements of H have the same heights in H as in G. An equivalent definition is that each coset modulo H contains an element of G such that this element has the same order in G as the coset has in G/H.

A subset $S = (a_\nu)$ of G, not containing 0, is said to be *independent* if for any finite subset $a_{\nu_1}, \ldots, a_{\nu_k}$ of S a relation

$$n_1 a_{\nu_1} + \cdots + n_k a_{\nu_k} = 0 \qquad (n_i \text{ integers})$$

implies $n_1 a_{\nu_1} = \cdots = n_k a_{\nu_k} = 0$, i. e. $O(a_{\nu_i}) | n_i$. The cardinal number of a maximal independent system of G is an invariant of G; it is called the *rank* of G, in notation: $\mathfrak{R}(G)$. It is immediate that if $\mathfrak{R}(G)$ is infinite, then it is equal to $|G|$.

Let $G^0 = G$ and define the subgroups G^α of G where α is an ordinal as follows: if $\alpha - 1$ exists then let G^α consist of all elements of $G^{\alpha-1}$ which are of infinite height in $G^{\alpha-1}$; if α is a limit ordinal then we define G^α as the meet of all G^β with $\beta < \alpha$. There is a least ordinal τ, not exceeding the power of G, satisfying $G^{\tau+1} = G^\tau$. This $\tau = \tau(G)$ is said to be the (*Ulm*) *type* of G. If G is reduced then $G^\tau = 0$. The factorgroups $G_\alpha = G^\alpha / G^{\alpha+1}$ are called the *Ulm factors* of G and the well-ordered sequence

$$G_0, G_1, \ldots, G_\alpha, \ldots \qquad (\alpha < \tau)$$

the *Ulm sequence* of G. No Ulm factor contains an element of infinite height and none of them is bounded, except possibly $G_{\tau-1}$ if this exists. It may readily be checked that $G_\alpha, G_{\alpha+1}, \ldots$ is the Ulm sequence of G^α and $G_0, \ldots, G_\beta, \ldots$ $(\beta < \alpha)$ is that of G/G^α.

The (discrete) direct sum of the groups A_ν will be written as $\sum_\nu A_\nu$; here ν is to be understood to range over an arbitrary set of indices.

As we have mentioned in the introduction, we shall need a generalization of the notion of direct sum. This concept which we shall call *interdirect sum*,[16] may be characterized as a group lying between the discrete and the complete direct sum, i. e. it is a subdirect sum containing each of its components. A set of postulates for interdirect sum is the following. A group G is called an interdirect sum of its subgroups A_ν if there are endomorphisms ε_ν of G such that (i) $\varepsilon_\nu G = A_\nu$; (ii) $\varepsilon_\nu \cdot \varepsilon_\mu = \varepsilon_\nu^2$ or 0 according as $\nu = \mu$ or

[15] In all cases it is evident which alternative is adequate.

[16] For this appropriate terminology the author is indebted to J. SURÁNYI.

$\nu \neq \mu$; (iii) $\varepsilon_\nu g = 0$ for every ν ($g \in G$) implies $g = 0$. It is easily seen that we get the discrete direct sum if $\varepsilon_\nu g \neq 0$ holds only for a finite number of endomorphisms ε_ν (g is fixed), and the complete direct sum if for any system of elements $a_\nu \in A_\nu$ there is a $g \in G$ such that $\varepsilon_\nu g = a_\nu$ for every ν.

An interdirect sum of the *finite* groups A_ν will be called a *restricted* interdirect sum if for any element $g \in G$ there is but a finite number of groups A_ν of the *same* order such that $0 \neq \varepsilon_\nu g \in A_\nu$. Evidently, then for a fixed g, there are only at most countable indices ν with $\varepsilon_\nu g \neq 0$.

Finally, we shall call an interdirect sum serving, if it is a serving subgroup of the complete direct sum.

§ 3. The basic subgroup and the quasibasis

1. The basic subgroup of an abelian p-group will play a fundamental role in our investigations. First of all we shall give a new proof for the existence of such a subgroup; the following proof seems to be somewhat simpler than KULIKOV's.[17]

Recall that by a *basic subgroup* of a p-group G is meant a subgroup B satisfying the following three conditions: (i) B is the direct sum of cyclic groups; (ii) B is a serving subgroup of G; (iii) the factorgroup G/B is algebraically closed.

THEOREM 1. (KULIKOV.) *Each abelian p-group G contains a basic subgroup.*

PROOF. Let us consider the elements of G which are of order p and select from this set a subset S_1 maximal with respect to the property of being independent but such that $\{S_1\}$ shall be a serving subgroup of G. Then we adjoin to S_1 elements of order p^2 in order to get a system S_2 maximal with respect to the property of being independent with the additional requirement that $\{S_2\}$ remain a serving subgroup of G. Thus proceeding, we obtain an ascending chain $S_1 \subseteq S_2 \subseteq \ldots$ of independent systems; let the union of this chain be denoted by S. We are going to show that $B = \{S\}$ is a basic subgroup of G.

Conditions (i) and (ii) are trivially satisfied, for independence and servingness are of inductive character. In order to verify (iii), it is plainly sufficient to prove that

$$px \equiv c \pmod{B} \tag{1}$$

has a solution $x \in G$ for each $c \notin B$. Suppose the contrary and let $c \notin B$ be an element in G of a possibly least order p^n for which (1) is not solvable Then $H(c) = 0$ and the reason why c does not belong to B is either that

[17] KULIKOV [8] and [9].

depends on S_n or is independent of S_n but $\{S_n, c\}$ is no longer a serving subgroup of G.

α) If c depends on S_n, then $p^{n-1}c \in B$ and, by the serving character of B, there is a $b \in B$ with $p^{n-1}c = p^{n-1}b$, i. e. $p^{n-1}(c-b) = 0$. Since $O(c-b) \leqq p^{n-1}$, the choice of c implies the existence of an x with $px \equiv c-b \equiv c \pmod{B}$.

β) If c is independent of S_n, then $\{S_n, c\}$ contains an element a such that

$$a = mc + m_1a_1 + \cdots + m_ka_k = p^s y \qquad (a_i \in S_n)$$

holds for some $y \in G$, but for no $y \in \{S_n, c\}$, i. e. not all of $m, m_1, \ldots, m_k$ are divisible by p^s. The serving character of $\{S_n\}$ implies $p^s \nmid m$ and therefore we may suppose $m = p^r < p^s$. Again by the servingness of $\{S_n\}$ we have $p^r | m_1, \ldots, p^r | m_k$, i. e.

$$p^r(c - p^{s-r}y + m_1'a_1 + \cdots + m_k'a_k) = 0 \qquad (m_i = p^r m_i').$$

Hence we conclude that there is some z with $pz \equiv c - p^{s-r}y + m_1'a_1 + \cdots + m_k'a_k \pmod{B}$ and so $x = z + p^{s-r-1}y$ satisfies (1).

The two contradictions complete the proof.

2. We remember that G may have several distinct basic subgroups, but *all basic subgroups must be isomorphic to each other* (cf. KULIKOV [8]).

3. Each basic subgroup gives rise to a special type of generating system which we shall need in the future. This generating system will be, in some respect, a substitute for the basis in groups which are no direct sums of cyclic groups.

By the definition of basic subgroups B, G/B is a complete p-group and therefore, it may be represented as the direct sum of quasicyclic groups,

$$G/B = \sum_\mu \bar{C}_\mu \cong \sum_\mu \mathfrak{Z}(p^\infty)$$

where $\bar{C}_\mu$ denotes a subgroup of G/B, generated by the cosets $\bar{c}_\mu^{(1)}, \bar{c}_\mu^{(2)}, \ldots$ connected by the relations

$$\bar{c}_\mu^{(1)} \neq \bar{0}, \quad p\bar{c}_\mu^{(1)} = \bar{0}, \quad p\bar{c}_\mu^{(2)} = \bar{c}_\mu^{(1)}, \quad p\bar{c}_\mu^{(3)} = \bar{c}_\mu^{(2)}, \ldots .$$

B being a serving subgroup of G, each coset modulo B may be represented in order preserving manner by elements, i. e. we have

$$(2) \qquad c_\mu^{(1)} \neq 0, \quad pc_\mu^{(1)} = 0, \quad pc_\mu^{(2)} = c_\mu^{(1)} - b_\mu^{(1)}, \quad pc_\mu^{(3)} = c_\mu^{(2)} - b_\mu^{(2)}, \ldots \quad (c_\mu^{(n)} \in \bar{c}_\mu^{(n)})$$

where $O(c_\mu^{(n)}) = p^n$ and

$$b_\mu^{(n)} = s_1^{(n)} a_{k_1}^{(n)} + \cdots + s_{k_m}^{(n)} a_{k_m}^{(n)} \in B \qquad (k_m \geqq 0,\ a_k^{(n)} \in B)$$

(a_ν denote the generators of the cyclic direct summands of B); and in addition, we may evidently assume the elements $c_\mu^{(n)}$ so to be chosen that

$$0 < s_i^{(n)} \leqq p-1.$$

It is immediate that G is generated by the elements

$$a_\nu, \quad c_\mu^{(n)} \qquad (n = 1, 2, \ldots)$$

where ν and μ range over appropriate sets of indices. In fact, for each element x of G, we may first represent the coset $\bar{x}=x+B$ in the form

$$\bar{x}=h_1\bar{c}_1^{(n_1)}+\cdots+h_s\bar{c}_s^{(n_s)} \qquad (h_i\not\equiv 0 \bmod p,\ s\geqq 0)$$

and then write

$$x-h_1c_1^{(n_1)}-\cdots-h_sc_s^{(n_s)}=r_1a_1+\cdots+r_ta_t \quad (\in B) \qquad (t\geqq 0)$$

to get the following expression

$$x=r_1a_1+\cdots+r_ta_t+h_1c_1^{(n_1)}+\cdots+h_sc_s^{(n_s)} \qquad (h_i\not\equiv 0 \bmod p). \tag{3}$$

The set consisting of all a_ν and $c_\mu^{(n)}$ will be called a *quasibasis* for G. This terminology may be justified by the fact that (3) is uniquely determined by the element x in the sense that all of $r_1a_1,\ldots,h_1c_1^{(n_1)},\ldots$ are unique.

4. With the help of this new notion one may easily prove

THEOREM 2. *If G is a reduced p-group and B is a basic subgroup of G, then*

$$|G|\leqq|B|^{\aleph_0}. \tag{4}$$

PROOF. It is clearly sufficient to show that in a quasibasis $a_\nu, c_\mu^{(n)}$ of $G(\neq 0)$ the power of all $c_\mu^{(1)}$ does not exceed $|B|^{\aleph_0}$ $(\geqq\aleph)$.[18] We first observe that each $c_\mu^{(1)}$ defines a sequence

$$b_\mu^{(1)},\ b_\mu^{(2)},\ldots \qquad (b_\mu^{(n)}\in B) \tag{5}$$

such that (2) holds. Now, if $c_\sigma^{(1)}(\neq c_\mu^{(1)})$ had the same sequence (5), then it would follow

$$p(c_\sigma^{(1)}-c_\mu^{(1)})=0,\quad p(c_\sigma^{(2)}-c_\mu^{(2)})=c_\sigma^{(1)}-c_\mu^{(1)},\quad p(c_\sigma^{(3)}-c_\mu^{(3)})=c_\sigma^{(2)}-c_\mu^{(2)},\ldots$$

contrary to the hypothesis that G is reduced, Therefore, the power of all $c_\mu^{(1)}$ can not be greater than the power of the set of all sequences (5), i. e. than $|B|^{\aleph_0}$.

We note that in (4) the sign of equality may well hold without being $|B|=|B|^{\aleph_0}$. In fact, if G is the torsion subgroup of the complete direct sum of the cyclic groups $\mathfrak{Z}(p), \mathfrak{Z}(p^2),\ldots$ then the discrete direct sum B of the same groups is readily seen to be a basic subgroup of G. Here $|G|=\aleph$ and $|B|=\aleph_0$, so that in (4) the sign of equality holds.

5. An interesting property of basic subgroups is established by

THEOREM 3.[19] *A basic subgroup B of G and a basic subgroup B_0 of the first Ulm factor $G_0=G/G^1$ of G are isomorphic.*

[18] $|B|\geqq 2$ for $G(\neq 0)$ is assumed to be reduced. ($\aleph$ denotes the power of the continuum.)

[19] Cf. KULIKOV [9], Theorem 4. 11.

PROOF. The obvious relation $B \cap G^1 = 0$, together with the first isomorphism theorem, leads us to the result

$$\{B, G^1\}/G^1 \simeq B/(B \cap G^1) \simeq B.$$

Hence, it suffices to verify that $B_0^* = \{B, G^1\}/G^1$ is a basic subgroup of G_0.[20] The stated isomorphism implies that B_0^* is the direct sum of cyclic groups, and since by the second isomorphism theorem $G_0/B_0^* = (G/G^1)/(\{B, G^1\}/G^1) \simeq G/\{B, G^1\}$ where the latter group is a homomorphic image of the complete group G/B, thus G_0/B_0^* is itself an algebraically closed group. What remains to be proved is the servingness of B_0^* in G_0. Let $p^n x \in \{B, G^1\}$, that is to say, $p^n x = b + g$ $(b \in B, g \in G^1)$. Since g is of infinite height, we obtain $g = p^n g'$ $(g' \in G)$, i. e., $p^n(x - g') = b$ whence, by the serving character of B in G, we have $p^n(x - g') = p^n b'$ $(b' \in B)$. We conclude $p^n x = p^n b' + g$ with $b' \in \{B, G^1\}$ and $g \in G^1$, completing the proof.

We mention as an obvious corollary to Theorem 3:

COROLLARY 1. *For a basic subgroup B and for the first Ulm factor G_0 of G we have*

$$|B| \leqq |G_0|.$$

Hence Theorem 2 implies

COROLLARY 2. *For a reduced p-group G and for its first Ulm factor G_0 we have*

$$|G| \leqq |G_0|^{\aleph_0}.$$

6. We shall have to make use of the following sharpening of Theorem 1.

THEOREM 4.[21] *Each p-group G contains a basic subgroup B satisfying*

$$\mathfrak{R}(G/B) = \min_{n=0,1,2,\ldots} \mathfrak{R}(p^n G). \tag{6}$$

PROOF. From the definition and existence of a quasibasis it results at once that the sign $>$ is impossible in (6). On the other hand, let B^* be an arbitrary basic subgroup of G and suppose that B^* does not fulfil condition (6):

$$\mathfrak{R}(G/B^*) < \mathfrak{R}(p^n G) \qquad \text{for } n = 0, 1, 2, \ldots$$

On account of the obvious isomorphism[22] $G/B^* \simeq p^n G/p^n B^*$ we have

$$\mathfrak{R}(p^n G/p^n B^*) < \mathfrak{R}(p^n G) \qquad \text{for } n = 0, 1, 2, \ldots$$

which implies

$$\mathfrak{R}(p^n B^*) = \mathfrak{R}(p^n G)$$

(observe that if B^* does not fulfil (6) then the rank of $p^n B^*$ can not be finite).

20 Here we make use of the fact mentioned in point **2** of this section.

21 See KULIKOV [9], Theorem 4. 24.

22 This isomorphism is an easy consequence of the construction of the quasibasis.

Let $B^* = \sum_\nu \{a_\nu\}$ and $\min_{n=0,1,2,\ldots} \mathfrak{R}(p^n G) = \min_{n=0,1,2,\ldots} \mathfrak{R}(p^n B^*) = \mathfrak{p}$. Then the power of the set of direct summands $\{a_\nu\}$ of order $> p^n$ is at least $\mathfrak{p}$ for each non-negative integer n, consequently, B^* can be represented as the direct sum of groups B^*_λ such that λ ranges over a set of power $\mathfrak{p}$ and each B^*_λ is the direct sum of cyclic groups of unbounded order:

$$B^*_\lambda = \sum_\varkappa \{a_{\lambda\varkappa}\} \qquad (O(a_{\lambda\varkappa}) = p^{n_{\lambda\varkappa}}).$$

Selecting an unbounded sequence $n_{\lambda 1} < n_{\lambda 2} < \cdots$, we form

$$B_\lambda = \{a_{\lambda 1} - p^{n_{\lambda 2} - n_{\lambda 1}} a_{\lambda 2},\ a_{\lambda 2} - p^{n_{\lambda 3} - n_{\lambda 2}} a_{\lambda 3}, \ldots\} + \sum_{\varkappa \neq 1, 2, \ldots} \{a_{\lambda\varkappa}\} =$$

$$= \{a_{\lambda 1} - p^{n_{\lambda 2} - n_{\lambda 1}} a_{\lambda 2}\} + \{a_{\lambda 2} - p^{n_{\lambda 3} - n_{\lambda 2}} a_{\lambda 3}\} + \cdots + \sum_{\varkappa \neq 1, 2, \ldots} \{a_{\lambda\varkappa}\}$$

and obtain[23] $B^*_\lambda / B_\lambda \cong \mathfrak{Z}(p^\infty)$. Now

$$B = \sum_\lambda B_\lambda$$

is a basic subgroup of B^* and hence also of G. Moreover, B satisfies (6) considering that

$$\mathfrak{R}(G/B) \geqq \mathfrak{R}(B^*/B) = \mathfrak{p} = \min_{n=0,1,\ldots} \mathfrak{R}(p^n G),$$

q. e. d. A basic subgroup B with property (6) will be called *strong*.

§ 4. p-groups without elements of infinite height

This section is devoted to a theorem that may be regarded as an analogue (but not a generalization)[24] of PRÜFER's famous theorem on countable p-groups without elements of infinite height. It is known that in the general case there is no direct decomposition, but the existence of an interdirect representation is ensured by the direct part of

THEOREM 5.[25] *A p-group G is isomorphic to a restricted and serving interdirect sum of cyclic groups if and only if it contains no elements of infinite height.*

PROOF. The "only if" part of our assertion is obvious, therefore we may restrict ourselves to the demonstration of the converse statement. Let us assume that G contains no elements of infinite height and take a quasibasis of G with elements a_ν, $c^{(n)}_\mu$. We shall show that G is isomorphic to a restricted and serving interdirect sum of the cyclic groups $\{a_\nu\}$.

[23] For a similar reasoning see KULIKOV [9], FUCHS [3], FUCHS, KERTÉSZ and SZELE [4].

[24] PRÜFER's theorem is no special case of Theorem 5. (For PRÜFER's theorem see PRÜFER [15], and for simpler proofs KULIKOV [7], [8] and KERTÉSZ [5].)

[25] An equivalent form of Theorem 5 is due to KULIKOV [8], § 5. Here we prefer to give an independent proof based on the notion of quasibasis.

Let $b_\mu^{(n)}$ have the same meaning as in (2). Then we assign to $c_\mu^{(1)}$ the following formal sum:

(7a) $$c_\mu^{(1)} \to b_\mu^{(1)} + p b_\mu^{(2)} + p^2 b_\mu^{(3)} + \cdots = m_{\mu 1}^{(1)} a_1 + m_{\mu 2}^{(1)} a_2 + \cdots$$

where on the right the terms are arranged with respect to the elements a_ν. Of course, this infinite sum contains but a countable number of non-zero terms. Similarly, let

(7b) $$\begin{aligned} c_\mu^{(2)} &\to b_\mu^{(2)} + p b_\mu^{(3)} + p^2 b_\mu^{(4)} + \cdots = m_{\mu 1}^{(2)} a_1' + m_{\mu 2}^{(2)} a_2' + \cdots \\ c_\mu^{(3)} &\to b_\mu^{(3)} + p b_\mu^{(4)} + p^2 b_\mu^{(5)} + \cdots = m_{\mu 1}^{(3)} a_1'' + m_{\mu 2}^{(3)} a_2'' + \cdots \\ &\cdots\cdots\cdots\cdots\cdots\cdots \end{aligned}$$

Then it is evident that these formal sums are connected by the same defining relations as the elements $c_\mu^{(1)}, c_\mu^{(2)}, \ldots$ themselves.

With the help of these sums we can assign to each element x of G a formal sum of finitely or countably many terms $m_\nu a_\nu \neq 0$, in the following manner. At first we represent x in its unique form (3) and then introduce in place of the $c_\mu^{(n)}$ their formal expressions given by (7a) and (7b); finally, we arrange the terms with respect to the elements a_ν. Let the totality of all formal sums thus arising be denoted by H.

If we define the addition for the elements of H in the obvious manner, then it is readily seen that the above correspondence between the elements of G and those of H is addition preserving; thus it is a homomorphism of G onto H. We have still to show that the kernel of this homomorphism is zero, i. e. that $x \to 0$ $(x \in G, 0 \in H)$ implies $x = 0$.

Let

(8) $$0 \neq x = h_1 c_1^{(n_1)} + \cdots + h_s c_s^{(n_s)} + r_1 a_1 + \cdots + r_t a_t \to 0 \quad (h_i \not\equiv 0 \bmod p);$$

then $s \geqq 1$, for $0 \neq x \in B$, $x \to 0$ is clearly impossible. As (8) implies $px \to 0$, $p^2 x \to 0, \ldots$, there is no loss of generality in assuming $n_1 = n_2 = \ldots = n_s = 1$, i. e.

(9) $$0 \neq x = h_1 c_1^{(1)} + \cdots + h_s c_s^{(1)} + r_1 a_1 + \cdots + r_t a_t \to 0 \qquad (0 < h_i \leqq p-1).$$

In view of the relations

$$p^n c_\mu^{(n+1)} = p^{n-1}(c_\mu^{(n)} - b_\mu^{(n)}) = p^{n-2}(c_\mu^{(n-1)} - b_\mu^{(n-1)}) - p^{n-1} b_\mu^{(n)} = \cdots$$
$$\cdots = c_\mu^{(1)} - b_\mu^{(1)} - p b_\mu^{(2)} - \cdots - p^{n-1} b_\mu^{(n)}$$

we have

$$x = p^n(h_1 c_1^{(n+1)} + \cdots + h_s c_s^{(n+1)}) + [(h_1 b_1^{(1)} + \cdots + h_s b_s^{(1)}) +$$
$$+ p(h_1 b_1^{(2)} + \cdots + h_s b_s^{(2)}) + \cdots + p^{n-1}(h_1 b_1^{(n)} + \cdots + h_s b_s^{(n)}) + r_1 a_1 + \cdots + r_t a_t] =$$
$$= p^n(h_1 c_1^{(n+1)} + \cdots + h_s c_s^{(n+1)}) + (k_1 a_1' + \cdots + k_q a_q').$$

The hypothesis $x \to 0$ as well as the fact that the formal sums satisfy exactly the same defining relations as the corresponding elements, imply that if we introduce here the above expressions for the $c_\mu^{(n+1)}$ and arrange with respect to the a_ν, then all terms vanish. Since in the first term of the last expression

the coefficients of the a_ν (in the non-vanishing terms) are all divisible by p^n, the same must be true for the second term, i. e.

$$k_1 a_1' + \cdots + k_q a_q' = p^n (k_1' a_1' + \cdots + k_q' a_q') = p^n y$$

for some $y \in G$. Consequently, $H(x) \geqq n$, and since this holds for each natural n, we are led to a contradiction to the fact that $x \neq 0$ must be of finite height in G. The definition of the formal sums shows that but a finite number of elements a_ν of the same order may occur in an infinite sum, so that this interdirect sum is actually restricted in the sense of § 2. The servingness of H in the complete direct sum follows easily: if $p^n z \in H$ holds for some z in the complete direct sum, then by the algebraic closure of H B there is some $x \in H$ with $p^n z - p^n x \in B$; hence for a suitable $b \in B$ we have $p^n(z-x) = p^n b$, in other words, $p^n z = p^n(x+b)$ with $x+b \in H$. Q. e. d.

A representation as restricted and serving interdirect sum of cyclic groups is unique in the following sense.

Theorem 6. *In the restricted and serving interdirect representations of a p-group G (without elements of infinite height) by means of cyclic groups the orders of the cyclic groups are uniquely determined.*

Proof. We show that the discrete direct sum B of the cyclic summands is a basic subgroup of G. Then by the isomorphism of all basic subgroups of a group, our assertion will follow at once.

The proof that B is a serving subgroup of G is so obvious that it may be left to the reader. What remains to be verified is the completeness of the factorgroup G/B, in other words, that each element g of G is of infinite height modulo B. If g contains infinitely many non-zero terms then, g being of finite order, there is but a finite number of these terms which are of height $< n$ for a fixed n. The sum of these terms is therefore an element of B, and so g is congruent modulo B to an element of the complete direct sum, and by the servingness, also to one of G, which is of height $\geqq n$, as we wished to prove.

§ 5. Necessary conditions for the Ulm sequence

Let G be a reduced p-group with the Ulm sequence G_α $(0 \leqq \alpha < \tau)$ where τ is an ordinal number not exceeding the power of G. For each α, we choose an arbitrary but fixed basic subgroup B_α of G_α, $B_\alpha = \sum_\nu \{a_{\alpha\nu}\}$.

Theorem 7. *For the Ulm sequence G_α $(\alpha < \tau)$ of the reduced p-group G the following conditions are satisfied:*

(I) $$\sum_{0 \leqq \alpha < \tau} |G_\alpha| \leqq |G| \leqq \prod_{0 \leqq \alpha < \min(\omega, \tau)} |G_\alpha|;$$

(II) $$\sum_{\beta \leqq \alpha < \tau} |G_\alpha| \leqq |G_\beta|^{\aleph_0} \qquad \textit{for all } 0 \leqq \beta < \tau;$$

(III) $$|B_{\alpha+1}| \leqq |p^n G_\alpha| \qquad \textit{for all } \alpha + 1 < \tau;\ n = 0, 1, 2, \ldots$$

PROOF. In (I), the first inequality is evident on account of the fact that the group G is the union of all (disjoint) sets $G^\alpha - G^{\alpha+1}$ for $0 \leqq \alpha < \tau$ ($G^\alpha - G^{\alpha+1}$ means the set of all elements of G^α not in $G^{\alpha+1}$), and clearly, $|G^\alpha - G^{\alpha+1}| \geqq |G^\alpha/G^{\alpha+1}| = |G_\alpha|$. In order to establish the second inequality, we may confine ourselves to the case $\omega \leqq \tau$, for otherwise an obvious equality holds. Let $\min\limits_{k=0,1,2,\ldots} |G_k| = |G_s|$. Then

$$|G| = |G/G^s|\,|G^s| = |G_0|\,|G_1| \ldots |G_{s-1}|\,|G^s|.$$

Applying Corollary 2 to the group G^s whose first Ulm factor is G_s, we obtain

$$|G^s| \leqq |G_s|^{\aleph_0} \leqq |G_s|\,|G_{s+1}| \ldots$$

whence the statement is trivial.

(II) may be verified at once, since for the group G^β we have by (I_1) and Corollary 2:

$$\sum_{\beta \leqq \alpha < \tau} |G_\alpha| \leqq |G^\beta| \leqq |G_\beta|^{\aleph_0}.$$

Now let us consider (III). The definition of $G^{\alpha+1}$ implies that for each natural integer n there must exist in $G^\alpha/G^{\alpha+2}$ a solution $x_\nu^{(n)}$ of the equation $p^n x_\nu^{(n)} = a_{\alpha+1,\nu}$. We show that $\nu \neq \mu$ implies $x_\nu^{(n)} \not\equiv x_\mu^{(m)}$ (mod $G^{\alpha+1}$). Indeed, from $x_\nu^{(n)} = x_\mu^{(m)} + a$ ($a \in G^{\alpha+1}/G^{\alpha+2} = G_{\alpha+1}$) it would follow (taking, say, $n \geqq m$) that

$$p^n \overset{\circ}{a} = p^n x_\nu^{(n)} - p^n x_\mu^{(m)} = a_{\alpha+1,\nu} - p^{n-m} a_{\alpha+1,\mu} \in B_{\alpha+1},$$

and so, by the serving property of $B_{\alpha+1}$, we would get

$$a_{\alpha+1,\nu} - p^{n-m} a_{\alpha+1,\mu} = p^n b \qquad (b \in B_{\alpha+1})$$

which is impossible in the basic subgroup $B_{\alpha+1}$. Taking into account that $x_\nu^{(n)}$ is of order p^n *modulo* $G^{\alpha+1}$, we arrive at the desired inequality. This completes the proof.

§ 6. The construction for groups of type ω

Condition (I) in the preceding theorem shows the remarkable fact that an upper estimation for the power of a group G may be given if one knows nothing else than the first ω Ulm factors of G. Therefore, it seems to be quite natural to discuss first of all the case $\tau = \omega$ separately. In fact, the general case can be reduced to this one. In case $\tau = \omega$ we find the following result.

THEOREM 8. *Let G_k ($k = 0, 1, 2, \ldots$) be a sequence of p-groups without elements of infinite height and $\mathfrak{p}$ a cardinal number satisfying*[28]

[28] We remark that the inequality

$$\sum_{k=n}^{\infty} |G_k| \leqq |G_n|^{\aleph_0}$$

corresponding to (II) in Theorem 7 is already a consequence of (ii) and of Theorem 2. In fact, $|G_{n+1}| \leqq |B_{n+1}|^{\aleph_0} \leqq |G_n|^{\aleph_0}$, $|G_{n+2}| \leqq |G_{n+1}|^{\aleph_0} \leqq |G_n|^{\aleph_0}$ etc. imply the desired inequality. (Here and in the theorem, B_k denotes a basic subgroup of G_k.)

(i) $$\sum_{k=0}^{\infty}|G_k|\leqq \mathfrak{p}\leqq \prod_{k=0}^{\infty}|G_k|;$$

(ii) $$|B_{k+1}|\leqq|p^n G_k| \qquad (n,k=0,1,2,\ldots).$$

Then there is a reduced p-group G of power $\mathfrak{p}$ and of type ω such that its Ulm sequence is just G_k $(k=0,1,2,\ldots)$.

PROOF. At first we define a group H of type ω and of power $\mathfrak{q}=\sum_{k=0}^{\infty}|G_k|(\leqq\mathfrak{p})$ with the Ulm factors G_k. For each k, we let correspond to the elements $a_{k\nu}$ and $c_{k\mu}^{(n)}$ of G_k (a quasibasis of G_k) generators $u_{k\nu}$ and $v_{k\mu}^{(n)}$ of H with the following set of defining relations:

1° $p^{n_{k\nu}}u_{k\nu}=0 \qquad$ (if $O(a_{k\nu})=p^{n_{k\nu}}$),

2° $pv_{k\mu}^{(1)}=u_{k+1,\nu}$,

3° $pv_{k\mu}^{(n+1)}=v_{k\mu}^{(n)}-s_1u_{k\nu_1}-\ldots-s_lu_{k\nu_l} \qquad (n\geqq 1)$

if and only if the (corresponding) relation

$$pc_{k\mu}^{(n+1)}=c_{k\mu}^{(n)}-s_1a_{k\nu_1}-\ldots-s_la_{k\nu_l}$$

holds in G_k.

We observe the important fact that if we take a quasibasis relative to a *strong* basic subgroup B_k, then the power of the set of all $c_{k\mu}^{(1)}$ for a fixed k is equal to $\min_{n=0,1,2,\ldots}\mathfrak{R}(p^nG_k)$ (cf. Theorem 4); consequently, p^nG_k being infinite, (ii) guarantees that the power of the set of all $u_{k+1,\nu}$ for a fixed k is not greater than $\mathfrak{R}(p^nG_k)$ and hence we may suppose that *in* 2° *every* $u_{k+1,\nu}$ *occurs* at least once.

Considering that each element x of H thus defined can be represented in the (unique) form

$$x=h_1u_{k_1\nu_1}+\cdots+h_ru_{k_r\nu_r}+l_1v_{k_1'\mu_1}^{(n_1)}+\cdots+l_tv_{k_t'\mu_t}^{(n_t)}$$

where $p\nmid l_i$ and $O(a_{k_i\nu_i})\nmid h_i$, it follows that H is a p-group. In order to see that this x does not collapse to 0 provided $r+t\geqq 1$, we map H into a group P of type p^∞ in the following manner: we map the element $u_{k\nu}$ upon an arbitrary element of order $p^{n_{k\nu}}$, or upon 0, then the image of $v_{k\mu}^{(1)}$ will be determined by using 2° and that of $v_{k\mu}^{(n+1)}(n\geqq 1)$ successively by the aid of 3°. (It must be noted that if the element on the right member of 2°, 3° is mapped upon $0\in P$, then the image of $v_{k\mu}^{(n+1)}$ can be taken arbitrarily of order p.) It is immediate that with this definition of mapping all defining relations of H are satisfied by the corresponding elements of P and therefore this mapping induces a homomorphism of H into P. Moreover, we may plainly choose the images of $u_{k\nu}$ and $v_{k\mu}^{(n)}$ so that the fixed element x is not mapped upon 0.[27] Hence $x\neq 0$, in fact. It also follows that H has the power $\mathfrak{q}$.

[27] It suffices to show this only for x with $n_1=\ldots=n_t=1$. If the image of a prescribed x of this type happens to be zero under some choice of mapping, then we alter

Next we turn to showing that $u_{k\nu}$ and $v_{k\mu}^{(n)}$ belong to G^k but not to G^{k+1}. This proposition is for $k=0$ quite evident and for $k \geqq 1$ we use induction. Let it be true for k. By 2^0 and 3^0, every $u_{k+1,\nu}$ is of infinite height in G^k (as $pv_{k\mu}^{(1)} = u_{k+1,\nu}$ implies $p^n v_{k\mu}^{(n)} = u_{k+1,\nu}$ by the construction of the quasibasis), i. e. $u_{k+1,\nu} \in G^{k+1}$. Further, each $v_{k+1,\mu}^{(n)}$ also belongs to G^{k+1}, for 3^0 implies

$$v_{k+1,\mu}^{(n)} = p^t v_{k+1,\mu}^{(n+t)} + h_1 u_{k+1,\nu_1} + \ldots + h_s u_{k+1,\nu_s}$$

and, as demonstrated just now, every $u_{k+1,\nu}$ is of infinite height in G^k. On the other hand, it is clear from the induction hypothesis that they are not of infinite height in G^{k+1}, i. e. they are not contained in G^{k+2}, q. e. d.

Knowing this, it is readily seen, by induction, from the arguments in the paragraph last but one as well as from the unicity of the quasibasis representation that no element of the form

$$(10) \qquad r_1 u_{k\nu_1} + \ldots + r_s u_{k\nu_s} + h_1 v_{k\mu_1}^{(n_1)} + \ldots + h_t v_{k\mu_t}^{(n_t)} \quad (p \nmid h_i,\ O(u_{k\nu_i}) \nmid r_i)$$

may belong to G^{k+1} (the corresponding element of G_k is of finite height!). Thus we infer that H is a group of type ω whose Ulm factors are G_k.

If in (i), $\mathfrak{q} = \mathfrak{p}$ holds, we are finished. If not, we proceed to define a group F of power $\prod_{k=0}^{\infty} |G_k| = \mathfrak{r}$ as the totality of all (finite and infinite)[28] vectors $w = (w_0, w_1, \ldots)$ where w_k (in the k-th place) is of the form (10) but such that the orders of w_k (considered as elements of H) are bounded (for a fixed w). In counting the sum $w + w'$ we agree to add componentwise but must always take into account that according to 2^0 we must put $pv_{k\mu}^{(1)} = u_{k+1,\nu}$ on the $k+1$-st place. Hence F is a p-group of power $\mathfrak{r}$ containing a subgroup H^* isomorphic to H; this H^* (which we shall henceforth identify with H itself) consists of all finite vectors w and an isomorphism between H^* and H may be given by $(w_0, w_1, \ldots) \leftrightarrow w_0 + w_1 + \ldots$.

It is evident that an element $(w_0, w_1, \ldots)$ of F is of infinite height (i. e. belongs to F^1) if and only if $w_0 = 0$. An easy induction leads us to the result that F^k consists of all vectors of the form $(0, 0, \ldots, 0, w_k, w_{k+1}, \ldots)$ whence the Ulm sequence of F is G_k $(k = 0, 1, 2, \ldots)$.

Let us turn our attention to the factorgroup F/H. Surely, it is of power $\mathfrak{r}$. Further, it is an algebraically closed group, for each coset modulo H may be represented by a vector of the form $(0, w_1, \ldots)$.

the mapping as follows: if x contains a $u_{k\nu}$ which is the p times of at most one $v_{k\mu}^{(1)}$ occurring in x, then we may alter the image of this $u_{k\nu}$ so that the image of x ceases to be zero; if such a $u_{k\nu}$ fails to exist, then we take an arbitrary $u_{k\nu}$ and choose zero for its image, finally, if necessary, we alter the image of exactly one of those $v_{k\mu}^{(1)}$ in x for which $pv_{k\mu}^{(1)}$ equals this $u_{k\nu}$. Thus the image of x will certainly be different from 0.

[28] We shall call a vector $w = (w_0, w_1, \ldots)$ *finite* if $w_k \neq 0$ for a finite number of indices k; otherwise it will be called an *infinite* vector.

Let G/H be a complete subgroup of F/H such that its power equals the given cardinal $\mathfrak{p}$. Then G is also of power $\mathfrak{p}$. In order to prove that the Ulm factors of G are just G_k, we show that $w=(w_0, w_1, \ldots)\in G$ belongs to G^k if and only if $w_0=\ldots=w_{k-1}=0$. The „only if" part of this statement follows from the trivial inclusion $F^k\supseteq G^k$, while the „if" part may be established by induction on k. Let $w=(0,0,\ldots,0,w_k,\ldots)\in G$; then, by the choice of G/H, we have $w\equiv p^n w'$ (mod H) for some $w'\in G$. Since together with $w'=(w_0', w_1', \ldots)$ also $w^*=(0,\ldots,0,w_k',\ldots)$ belongs to G, one has $w=p^n w^*+w''$ with $w''\in H$. Take into account that by induction hypothesis $w^*\in G^{k-1}$ and besides $w''\in H^k$, so that $w\in G^k$, indeed. Consequently, G has the Ulm sequence G_k, i. e. G is a group with the prescribed properties, q. e. d.

REMARKS. 1. Of course, Theorem 8 also holds for groups whose type is a finite ordinal. Then there is no choice for the power of the group, for the lower and upper bounds in (I) coincide.

2. We note that even in case $\mathfrak{q}=\mathfrak{p}$ we may take — although it seems to be superfluous — infinite vectors in G by choosing for G/H, as above, a complete subgroup of F/H of power $\mathfrak{p}$. This is always possible if $\mathfrak{q}<\mathfrak{r}$. It is readily seen that in the case $\mathfrak{q}=\mathfrak{r}$ the same is true with $\mathfrak{p}^*=\min_k |G_k|^{\aleph_0}$ in place of $\mathfrak{p}$.

3. For future purposes it must be noted that H is a serving subgroup of F. In fact, if $p^n w$ is a finite vector then $p^n w-p^n(w_0,0,0,\ldots)$ is a finite vector of infinite height in H whence the statement is immediate. Therefore, each coset modulo H may be represented by an element of G in an order preserving manner. Representing in this manner a maximal independent coset system of order p (taken modulo H, of course), we get again an independent system of infinite vectors, of the same power, which are easily seen to be independent modulo H too: if a linear combination of them lies in H, then all terms vanish. Consequently, there is no loss of generality in assuming that G contains a modulo H independent system of infinite vectors of order p whose power is $\mathfrak{p}^*$ (cf. the preceding remark).

4. It is easy to describe all elements of order p in G provided in 2° each $u_{k+1,\nu}$ occurs no more than once. If $pw=0$ for some $w=(w_0, w_1, \ldots)\in G$, then none of w_k may contain either a $v_{k\mu}^{(n)}$ with $n>1$ (this is trivial) or one with $n=1$, considering that we have agreed in putting $pv_{k\mu}^{(1)}=u_{k+1,\nu}$ and $u_{k+1,\nu}$ can not vanish in the $k+1$-st place of pw. Thus $pw=0$ if and only if for every k we have $pw_k=0$ and w_k contains none of $v_{k\mu}^{(n)}$. — Without making the assumption on 2° one can prove by the same arguments that $p(w_0, w_1, \ldots, w_k, \ldots)=0$ implies $p(0,0,\ldots,w_k, w_{k+1}, \ldots)=0$.

§ 7. The construction of groups with a prescribed Ulm sequence

Now we are ready to solve the problem of constructing a p-group G of a given type and power and with a given Ulm sequence. The result is as follows:

THEOREM 9. *Let $\mathfrak{p}$ be a cardinal, τ an ordinal number and G_α $(0 \leqq \alpha < \tau)$ a sequence of non-trivial p-groups without elements of infinite height such that*

(I*) $$\sum_{0 \leqq \alpha < \tau} |G_\alpha| \leqq \mathfrak{p} \leqq \prod_{0 \leqq \alpha < \min(\omega, \tau)} |G_\alpha|;$$

(II*) $$\sum_{\beta \leqq \alpha < \tau} |G_\alpha| \leqq |G_\beta|^{\aleph_0} \qquad \textit{for all } 0 \leqq \beta < \tau;$$

(III*) $$|B_{\alpha+1}| \leqq |p^n G_\alpha| \qquad \textit{for all } \; 1 \leqq \alpha+1 < \tau; \; n = 0, 1, 2, \ldots$$

where $B_{\alpha+1}$ is a basic subgroup of $G_{\alpha+1}$. Then there is a reduced p-group G satisfying

a) $|G| = \mathfrak{p}$,

b) $\tau(G) = \tau$,

c) *the Ulm sequence of G is G_α $(0 \leqq \alpha < \tau)$.*

PROOF. First of all we write the given ordinal number τ in the (unique) form

$$\tau = \omega\sigma + r$$

(σ an ordinal, r a non-negative integer). Then we break up the sequence G_α into the following well-ordered sequence of sequences of type ω:

(11) $$G_\gamma \quad \text{with} \quad \omega\varrho \leqq \gamma < \omega(\varrho+1) \quad (\text{resp. } \omega\sigma \leqq \gamma < \omega\sigma + r)$$

where $0 \leqq \varrho < \sigma$ and the last sequence — if it exists at all — may be finite (this is the case if $r > 0$).

For each ϱ we shall construct a group K_ϱ of type [29] ω with the Ulm sequence (11). Let $\mathfrak{p}_0 = |K_0| = \mathfrak{p}$ and

(12) $$\mathfrak{p}_\varrho = |K_\varrho| = \sum_{\omega\varrho \leqq \alpha < \tau} |G_\alpha| \qquad (\text{for } \varrho > 0).$$

Of course, (III*) implies (ii) in Theorem 8, and (II*) implies

$$\mathfrak{p}_\varrho = \sum_{\omega\varrho \leqq \alpha < \beta} |G_\alpha| + \sum_{\beta \leqq \alpha < \tau} |G_\alpha| \leqq \sum_{\omega\varrho \leqq \alpha < \beta} |G_\alpha| + |G_\beta|^{\aleph_0} \leqq \prod_{\omega\varrho \leqq \gamma < \omega(\varrho+1)} |G_\gamma|$$

(we have put $|G_\beta| = \min_{\omega\varrho \leqq \gamma < \omega(\varrho+1)} |G_\gamma|$) so that $\mathfrak{p}_\varrho$ fulfils (i). Consequently, by Theorem 8, a p-group K_ϱ of power $\mathfrak{p}_\varrho$ with the stated properties exists for all ϱ with $0 \leqq \omega\varrho < \tau$.

In each group K_ϱ we take a quasibasis $b_{\varrho\nu}, d_{\varrho\mu}^{(n)}$ such that for the basic subgroup of K_ϱ we choose the set of all vectors $(w_0, 0, 0, \ldots)$ where w_0 lies in the group $\{u_{01}, \ldots, u_{0\nu}, \ldots\}$ (corresponding to the basic subgroup of the first Ulm factor $G_{\omega\varrho}$ of K_ϱ; cf. Theorem 3). We proceed to define a group G as follows. For every ϱ, we take generator elements $y_{\varrho\nu}$ and $z_{\varrho\mu}^{(n)}$ corresponding to $b_{\varrho\nu}$ and $d_{\varrho\mu}^{(n)}$, respectively, with the defining relations

[29] For the last sequence in (11) — if it exists and is finite — the following construction is by § 6 obvious and therefore it needs no separate discussion.

1° $p^{n_{\varrho\nu}} y_{\varrho\nu} = 0$ (if $O(b_{\varrho\nu}) = p^{n_{\varrho\nu}}$),

2° $pz^{(1)}_{\varrho\mu} = \begin{cases} 0 & \text{or} \\ y_{\varphi\nu} & \text{with } \varphi > \varrho, \text{ or } 0 \end{cases}$

according as $d^{(1)}_{\varrho\mu}$ is a finite or infinite vector in K_{ϱ},.

3° $pz^{(n+1)}_{\varrho\mu} = z^{(n)}_{\varrho\mu} - s_1 y_{\varrho\nu_1} - \dots - s_l y_{\varrho\nu_l}$ $(n \geqq 1)$

if and only if

$pd^{(n+1)}_{\varrho\mu} = d^{(n)}_{\varrho\mu} - s_1 b_{\varrho\nu_1} - \dots - s_l b_{\varrho\nu_l}$

holds in K_{ϱ}.

Let us remark what follows.

1. By Remark 3 in § 6, the group K_{ϱ} may be assumed to contain $\mathfrak{p}^*_{\varrho}$ infinite modulo H independent vectors of order p, therefore, we may suppose that the set of all $d^{(1)}_{\varrho\nu}$ contains $\mathfrak{p}^*_{\varrho}$ infinite vectors which are independent modulo finite vectors. (We have put $\mathfrak{p}^*_{\varrho} = \min\limits_{\omega\varrho \leqq \gamma < \omega(\varrho+1)} |G_{\gamma}|^{\aleph_0}$.)

2. The set of all $y_{\varphi\nu}$ with $\varphi > \varrho$ has (by Theorem 3) the power (cf. (II*))

$$\sum_{\varrho<\varphi} |B_{\omega\varphi}| \leqq \sum_{\varrho<\varphi} |G_{\omega\varphi}| \leqq \sum_{\beta \leqq \alpha < \tau} |G_{\alpha}| \leqq |G_{\beta}|^{\aleph_0} = \mathfrak{p}^*_{\varrho}; \left(|G_{\beta}| = \min_{\omega\varrho \leqq \gamma < \omega(\varrho+1)} |G_{\gamma}|\right),$$

consequently, by our first remark, we may assume that *in* 2°, *for every fixed* ϱ, *all* $y_{\varphi\nu}$ *with* $\varphi > \varrho$ *occur at least once, but only for the independent vectors.*

3. The defining relations as given above imply that the element corresponding to a *finite* vector of order p is again of order p. Thus if $pz^{(1)}_{\varrho\mu} = y_{\varphi\nu}$ then not only $d^{(1)}_{\varrho\mu}$ has the property that p times of its corresponding element is $y_{\varphi\nu}$, but also each vector which differs from $d^{(1)}_{\varrho\mu}$ by a finite vector of order p. In particular, together with $d^{(1)}_{\varrho\mu} = (w_0, w_1, \dots)$ also $(0, \dots, 0, w_k, w_{k+1}, \dots)$ has the mentioned property, i. e. not only K_{ϱ} itself, but also all K^k_{ϱ} $(k = 0, 1, \dots)$ have the property of containing an element w such that $y_{\varphi\nu}$ corresponds to pw.

Now, we are going to show that the group G generated by all elements $y_{\varrho\nu}, z^{(n)}_{\varrho\mu}$ satisfies all conditions enumerated in the theorem.

That G is a p-group is quite obvious. The next step is the observation that each element g of G may be written (uniquely) in the form

$$g = h_1 y_{\varrho_1\nu_1} + \dots + h_s y_{\varrho_s\nu_s} + l_1 z^{(n_1)}_{\chi_1\mu_1} + \dots + l_t z^{(n_t)}_{\chi_t\mu_t}$$

with $p \nmid l_i$ and $O(b_{\varrho_i\nu_i}) \nmid h_i$, further, that entirely in the same way as described in the preceding section we can show that g is never zero unless it is trivially zero, i. e. $s = t = 0$.

Hence it results at once that $|G| = \mathfrak{p}$. In fact, as the first inequality in (I*) implies that $\mathfrak{p}_{\varrho} \leqq \mathfrak{p}$ for each ϱ and that the power of τ is at most $\mathfrak{p}$, we obtain

$$\mathfrak{p} \leqq |G| = \sum_{\varrho} \mathfrak{p}_{\varrho} \leqq \mathfrak{p}\mathfrak{p} = \mathfrak{p}.$$

We have still to prove that G has the Ulm sequence G_{α} $(0 \leqq \alpha < \tau)$. To this end we show, first of all, that $y_{\varrho\nu}$ and $z^{(n)}_{\varrho\mu}$ belong to G^1 for $\varrho \geqq 1$.

For the same reason as in the preceding section it follows that this assertion must be verified only for $y_{\varrho\nu}$. But this is an immediate consequence of 2° and the second remark. Further, remark 3 implies that they belong to all G^k (with $k=2,3,\ldots$), i. e. to G^ω. Therefore, the first ω Ulm factors of G are actually $G_0, G_1, \ldots$. A similar reasoning completes the proof that G is a desired group.

By Theorems 7 and 9 we arrive at the following result:

THEOREM 10. *Conditions* (I*)—(III*) *are necessary and sufficient for the existence of a reduced p-group G of power $\mathfrak{p}$, type τ and with the Ulm sequence G_α* $(0 \leqq \alpha < \tau)$.

It we put $\mathfrak{p}=\aleph_0$, we reget ZIPPIN's theorem.

§ 8. Some conclusions

Theorem 9 enables us to give examples showing that ULM's theorem does not hold for groups of power $\geqq \aleph_1$.

Let $G_0, G_1, \ldots, G_k, \ldots$ be a sequence (of type ω) of unbounded countable p-groups without elements of infinite height. Then, by PRÜFER's theorem, they are their own basic subgroups, hence (III*) and, trivially, (II*) are fulfilled. If we choose firstly $\mathfrak{p}=\aleph_0$ and secondly $\mathfrak{p}=\aleph_1$, then (I*) is also satisfied in both cases. Consequently, by Theorem 9, there exist groups G and G' of power $\aleph_0$ and $\aleph_1$, respectively, whose types $(=\omega)$ and Ulm sequences $(=G_k)$ are the same, without the groups themselves being isomorphic.

It is not difficult to show by an instance that it may happen also for groups of the same power $\mathfrak{p}$, where $\mathfrak{p} \geqq \aleph_1$, that they are of the same type and have the same Ulm sequence, however, they fail to be isomorphic. Let

$$G_0, G_1, \ldots, G_\omega, G_{\omega+1}, \ldots$$

be a sequence of type $\omega 2$ where G_α $(1 \leqq \alpha < \omega 2)$ are unbounded countable p-groups and G_0 is an arbitrary unbounded p-group of power $\mathfrak{p}$; no G_α contains elements of infinite height. By Theorem 8 there exist groups G^* and G^{**} of type ω and of power $\mathfrak{p}$ and $\aleph_0$, respectively, whose Ulm sequences are $G_0, G_1, \ldots, G_k, \ldots$ and $G_\omega, G_{\omega+1}, \ldots, G_{\omega+k}, \ldots$ respectively. As in the proof of Theorem 9, one may establish the existence of a reduced p-group G of type $\omega 2$ for which $G/G^\omega \cong G^*$ and $G^\omega \cong G^{**}$. This G is of power $\mathfrak{p}$ and has the prescribed Ulm sequence. On the other hand, if we construct another reduced group G' in the same way with the sole modification that we require $|G^{**}|=\aleph_1$, then G and G' yield a sought pair of reduced groups. These examples inform us that ULM's theorem ceases to hold even for groups of power $\geqq \aleph_1$.

The latter instance may suggest that perhaps ULM's theorem — which is a surprisingly deep result in the light of the proof of ZIPPIN's theorem, for there is a great variety of ways of giving the defining relations, and iso-

morphism will still hold — keeps its validity if besides the power of G one is given also the powers of all subgroups G^α of G (of course, satisfying certain postulates). [Evidently, in the countable case one may consider the powers of G^α to be also known.] The next example[30] will serve to demonstrate that the knowledge of these powers is not yet sufficient for the isomorphisms of the groups.

Let G_0 be the torsion subgroup of the complete direct sum of the groups $\mathfrak{Z}(p), \mathfrak{Z}(p^2), \ldots$, and let G_1 be the direct sum of cyclic groups of order p such that $|G_1| = \aleph$. We take the discrete direct sum of the cyclic groups in G_0 in order to get a basic subgroup B_0 of G_0, $B_0 = \sum_{k=1}^{\infty} \{a_{0k}\}$, and then complete the system (a_{0k}) by the elements $c_{0\mu}^{(n)}$ to obtain a quasibasis for G_0. In view of § 6, there is a reduced p-group G, defined by the elements $u_{0k}, v_{0\mu}^{(n)}, u_{1\nu}$ connected by the relations 1^0—3^0, such that the Ulm factors of G are G_0 and $G_1 = \sum_\nu \{a_{1\nu}\}$.[31] We may also construct another group G', again with the Ulm factors G_0 and G_1, and with the same generator elements, but we somewhat alter the defining relations 1^0—3^0 by requiring that in 2^0 not necessarily $pv_{0\mu}^{(1)} = u_{1\nu}$ but either $pv_{0\mu}^{(1)} = u_{1\nu}$ or $=0$, and both relations hold for a set of elements $v_{0\mu}^{(1)}$ of power $\aleph$. The groups G, G' are of power $\aleph$, of type 2 and have the same Ulm sequence G_0, G_1; however, they are not isomorphic. For, if we take into consideration the factorgroups G_*/G_1 and G'_*/G_1 where G_*, G'_* are the set of all elements of G, G' whose orders are $\leqq p$, then it follows by an easy inference that $|G_*/G_1| = \aleph_0$, while $|G'_*/G_1| = \aleph$. In fact, the first factorgroup is generated by the elements u_{0k} and the second factorgroup besides these elements also by those $v_{0\mu}^{(1)}$ for which in 2^0, $pv_{0\mu}^{(1)} = 0$ holds (cf. Remark 4 in § 6).

To sum up, countability is a heavy restriction and if we remove it, quite another situation arises from the group-theoretical point of view. The characterization of the reduced p-groups of arbitrary power by means of invariants seems to be an extraordinarily difficult problem.

Note *(added 28 August 1953).* The continuation of Kulikov's paper has now appeared (Обобщенные примарные группы. II, Труды Моск. Мат. Общ., 2 (1953), pp. 85—167). Conditions (I*)—(III*) and those obtained by Kulikov differ only in condition (III*) whose analogue in Kulikov's main theorem 10. 1 is condition (s_2) $|G_{\alpha+1}/pG_{\alpha+1}| \leq \Re(p^\omega G_\alpha)$. It is easy to show that (s_2) and (III*) are equivalent. In fact, the isomorphism $G_{\alpha+1}/pG_{\alpha+1} \simeq B_{\alpha+1}/pB_{\alpha+1}$ implies $|B_{\alpha+1}| = |B_{\alpha+1}/pB_{\alpha+1}| = |G_{\alpha+1}/pG_{\alpha+1}|$ and besides we have clearly $\Re(p^\omega G_\alpha) = |p^\omega G_\alpha|$ (provided the groups are infinite which can be supposed for otherwise the assertion is obvious). — Several preparatory

[30] The idea of this instance originates from an example given by Kulikov; see Kurosh [13].

[31] We assume that each $u_{1\nu}$ occurs in 2^0 exactly once.

theorems are similar and the two proofs have also the analogy in that they are carried out in two steps, but the principal ideas on which the proofs are based are quite different.

(Received 2 July 1953)

Bibliography

[1] R. Baer, The subgroup of the elements of finite order of an abelian group, *Annals of Math.*, (2), **37** (1936), pp. 766—781.
[2] D. Derry, Über eine Klasse von Abelschen Gruppen, *Proc. London Math. Soc.*, **43** (1937), pp. 490—506.
[3] L. Fuchs, The direct sum of cyclic groups, *Acta Math. Acad. Sci. Hung.*, **3** (1952), pp. 177—195.
[4] L. Fuchs, A. Kertész and T. Szele, Abelian groups in which every serving subgroup is a direct summand, *Publicationes Math. (Debrecen)*, **3** (1954) (under press).
[5] A. Kertész, On the decomposibility of abelian p-groups into the direct sum of cyclic groups, *Acta Math. Acad. Sci. Hung.*, **3** (1952), pp. 121—126.
[6] A. Kertész and T. Szele, On abelian groups every multiple of which is a direct summand, *Acta Sci. Math. (Szeged)*, **14** (1952), pp. 157—166.
[7] Л. Я. Куликов, К теории абелевых групп произвольной мощности, Матем. Сборник, **9** (51) (1941), pp. 165—181.
[8] Л. Я. Куликов, К теории абелевых групп произвольной мощности, Матем. Сборник, **16** (58) (1945), pp. 129—162.
[9] Л. Я. Куликов, Обобщенные примарные группы. I, Труды Моск. Мат. Общ., **1** (1952), pp. 247—326.
[10] A. Kurosch, Zur Zerlegung unendlicher Gruppen, *Math. Annalen*, **106** (1932), pp. 107—113.
[11] A. Kurosch, Primitive torsionsfreie abelsche Gruppen vom endlichen Range, *Ann. of Math.*, (2), **38** (1937), pp. 175—203.
[12] А. Г. Курош, Теория групп (Москва, 1944), 1st ed.
[13] А. Г. Курош, Теория групп (Москва, 1953), 2nd ed.
[14] А. И. Мальцев, Абелевы группы конечного ранга без кручения, Матем. Сборник, **4** (46) (1938), pp. 45–68.
[15] H. Prüfer, Untersuchungen über die Zerlegbarkeit der abzählbaren primären Abelschen Gruppen, *Math. Zeitschrift*, **17** (1923), pp. 35—61.
[16] T. Szele and J. Szendrei, On abelian groups with commutative endomorphism ring, *Acta Math. Acad. Sci. Hung.*, **2** (1951), pp. 309—324.
[17] T. Szele, Ein Analogon der Körpertheorie für Abelsche Gruppen, *Journ. f. reine u. angew. Math.*, **188** (1950), pp. 167—192.
[18] T. Szele, On non-countable abelian p-groups, *Publicationes Math. (Debrecen)*, **2** (1952), pp. 300—301.
[19] H. Ulm, Zur Theorie der abzählbar-unendlichen Abelschen Gruppen, *Math. Ann.*, **107** (1933), pp. 774—803.
[20] H. Ulm, Zur Theorie der nicht-abzählbaren primären Abelschen Gruppen, *Math. Zeitschrift*, **40** (1935), pp. 205—207.
[21] L. Zippin, Countable torsion groups, *Ann. of Math.*, (2), **36** (1935), pp. 86—99.

О СТРОЕНИИ ПРИМАРНЫХ АБЕЛЕВЫХ ГРУПП

Л. ФУКС (Будапешт)

(Резюме)

Вопрос о строении примарных абелевых групп наименьшей бесконечной, т. е. счетной мощности был решен почти двадцать лет тому назад: знаменитые теоремы Прюфера, Ульма и Циппина дают полную характеристику этих групп с помощью целочисленных инвариантов. При рассмотрении p-групп произвольной мощности встречаются значительные трудности; многие из них были отстранены Куликовым. Автор рассматривает теоремы для p-групп произвольной мощности, аналогичные теоремам Прюфера, Ульма и Циппина.

Доказывается следующая теорема, соответствующая теореме Прюфера и эквивалентная одной теореме Куликова:

Абелева p-группа, не содержащая элементов бесконечной высоты, изоморфна некоторой междупрямой сумме циклических p-групп; порядки прямых слагаемых определены при этом однозначно. (Мы называем междупрямой суммой такую группу, которая лежит между дискретной и полной прямыми суммами.)

В самое последнее время Куликову удалось найти теорему, соответствующую теореме Циппина. Не зная об этом результате Куликова, автор тоже решил проблему обобщения теоремы Циппина; основная идея приведенного здесь метода существенно отличается от метода Куликова и дает более непосредственное доказательство, так как Куликов доказывает свою теорему в более общей форме. Теорема гласит:

Пусть заданы кардинальное число $\mathfrak{p}$, порядковое число τ и вполне упорядоченная последовательность (типа τ) p-групп $G_\alpha \, (0 \leqq \alpha < \tau)$ не содержащих элементов бесконечной высоты. Для того, чтобы существовала редуцированная p-группа G мощности $\mathfrak{p}$ и типа τ, ульмовской последовательностью которой является как раз G_α, необходимо и достаточно, чтобы выполнялись следующие условия:

$$\sum_{0 \leqq \alpha < \tau} |G_\alpha| \leqq \mathfrak{p} \leqq \prod_{0 \leqq \alpha < \min(\omega, \tau)} |G_\alpha|; \tag{1}$$

$$\sum_{\beta \leqq \alpha < \tau} |G_\alpha| \leqq |G_\beta|^{\aleph_0} \quad \text{для} \quad 0 \leqq \beta < \tau; \tag{2}$$

$$|B_{\alpha+1}| \leqq |p^n G_\alpha| \quad \text{для} \quad 1 \leqq \alpha + 1 < \tau; \ n = 0, 1, 2, \ldots \tag{3}$$

где $B_{\alpha+1}$ базисная подгруппа группы $G_{\alpha+1}$.

Используя это обобщение теоремы Циппина, можно привести простые примеры, показывающие, что уже для групп мощности $\aleph_1$ теорема Ульма не имеет места.

ON IDEAL-QUOTIENTS AND PRIME IDEALS

By
OTTO STEINFELD (Szeged)
(*Presented by* L. RÉDEI)

§ 1. Introduction

First of all we introduce the following notions: Suppose in the (associative but not necessarily commutative) ring R we are given a subset H and a (twosided) ideal $\mathfrak{b}$. The elements β of R satisfying

(1) $$\beta H \subseteqq \mathfrak{b}$$

form a left ideal in R,[1] which we shall call a left ideal-quotient and denote by $(\mathfrak{b}:H)_l$. In a similar way, the right ideal-quotient $(\mathfrak{b}:H)_r$ is formed by the elements β satisfying

(2) $$H\beta \subseteqq \mathfrak{b}.$$

$(\mathfrak{b}:H)_r$ is of course a right ideal in R. The set of all elements β, satisfying (1) and (2) at the same time, will be called ideal-quotient and denoted by $\mathfrak{b}_H = \mathfrak{b}:H$.[2] Evidently we have $\mathfrak{b} \subseteqq \mathfrak{b}:H$, $(\mathfrak{b}:H)_l$, $(\mathfrak{b}:H)_r$, and

(3) $$\mathfrak{b}_H = \mathfrak{b}:H = (\mathfrak{b}:H)_l \cap (\mathfrak{b}:H)_r.$$

In particular, if $H = \mathfrak{b}$, we have $\mathfrak{b}:\mathfrak{b} = R$. In case R is commutative, obviously $(\mathfrak{b}:H)_l = (\mathfrak{b}:H)_r = \mathfrak{b}:H$ holds, and $\mathfrak{b}:H$ coincides with the classical notion of ideal-quotient.

In this paper we shall consider in the first place the cases where H is an ideal, a one-sided ideal or an element of a given ideal.

As usual, we call the ideal $\mathfrak{p}$ of R a *prime ideal*, if $\mathfrak{a}\mathfrak{b} \subseteqq \mathfrak{p}$ ($\mathfrak{a}, \mathfrak{b}$ ideals in R) implies $\mathfrak{a} \subseteqq \mathfrak{p}$ or $\mathfrak{b} \subseteqq \mathfrak{p}$. As it has been proved by N. H. MCCOY ([1] Theorem 1), a prime ideal can be defined also in the following equivalent

[1] This statement follows from the fact that $\varrho H \subseteqq \mathfrak{b}$ and $\sigma H \subseteqq \mathfrak{b}$ imply $(\varrho - \sigma) H \subseteqq \mathfrak{b}$ and $R\varrho H \subseteqq \mathfrak{b}$. If, specially, H is a (left) ideal in R, $\varrho R H \subseteqq \mathfrak{b}$ is also fulfilled, so $(\mathfrak{b}:H)_l$ is now an ideal.

[2] If $H = \mathfrak{a}$ is an ideal in R, $\mathfrak{b}:\mathfrak{a}$ is evidently also an ideal in R. In the case of an arbitrary set H, the ideal-quotient $\mathfrak{b}_H$ is a module such that $R\mathfrak{b}_H \cap \mathfrak{b}_H R \subseteqq \mathfrak{b}_H$ is also fulfilled. (A submodule M of R satisfying $MR \cap RM \subseteqq M$ may be called a quasi-ideal. We hope to consider quasi-ideals on a later occasion.)

[3] Cf. e. g. B. L. VAN DER WAERDEN, *Moderne Algebra*, vol. II. (Berlin, 1931), § 81.

ways: The ideal $\mathfrak{p}$ is a prime ideal if one of the following conditions is fulfilled:

a) if (α), (β) are any principal ideals in R satisfying $(\alpha)(\beta)\subseteq\mathfrak{p}$, then we have $(\alpha)\subseteq\mathfrak{p}$ or $(\beta)\subseteq\mathfrak{p}$;

b) if α, β are elements of R such that $\alpha R\beta\subseteq\mathfrak{p}$, then we have $\alpha\in\mathfrak{p}$ or $\beta\in\mathfrak{p}$;

c) if $\mathfrak{l}_1, \mathfrak{l}_2$ are any left ideals in R satisfying $\mathfrak{l}_1\mathfrak{l}_2\subseteq\mathfrak{p}$, then we have $\mathfrak{l}_1\subseteq\mathfrak{p}$ or $\mathfrak{l}_2\subseteq\mathfrak{p}$;

d) if $\mathfrak{r}_1, \mathfrak{r}_2$ are any right ideals in R satisfying $\mathfrak{r}_1\mathfrak{r}_2\subseteq\mathfrak{p}$, then we have $\mathfrak{r}_1\subseteq\mathfrak{p}$ or $\mathfrak{r}_2\subseteq\mathfrak{p}$.

The ideal $\mathfrak{q}$ will be called a *complete prime ideal* if $\alpha\beta\in\mathfrak{q}$ $(\alpha, \beta\in R)$ implies $\alpha\in\mathfrak{q}$ or $\beta\in\mathfrak{q}$.

Comparing the definition of the complete prime ideal with *a)*, it is obvious that a complete prime ideal is always a prime ideal, the converse being generally false. Further, it is easy to see that in case of a commutative ring the two notions coincide.[4]

Naturally, the ring R itself is always a complete prime ideal (and so a prime ideal). We shall call the ideal $\mathfrak{a}$ of R a *proper* ideal, if $R\neq\mathfrak{a}$.

In his paper [2] M. NAGATA has proved — among others — the following theorem:

Let S be a subring of the ring R and $\mathfrak{p}_1$ a prime ideal in S. Then there exists a prime ideal $\mathfrak{p}$ in R such that $\mathfrak{p}\cap S=\mathfrak{p}_1$ if (and only if) there exists an ideal $\mathfrak{a}$ in R such that $\mathfrak{a}\cap S=\mathfrak{p}_1$. The last condition is satisfied if S is an ideal in R.

REMARK I. When S is an ideal in R and $\mathfrak{p}_1\neq S$, no ideal properly containing $\mathfrak{p}$ has the property in our assertion.

REMARK II. It follows that every semi-prime ideal in S is an ideal in R if S is an ideal in R.[5]

In this paper we treat the case when S is an ideal in R. We show that the ideal-quotient $\mathfrak{p}_1:S$ is a prime ideal $\mathfrak{p}$ occurring in NAGATA's theorem. Further, we show that, if $\mathfrak{p}_1\neq S$, the prime ideal $\mathfrak{p}$ satisfying $S\cap\mathfrak{p}=\mathfrak{p}_1$ is unique. This can be expressed in the form $\mathfrak{p}=(\mathfrak{p}_1:\mathfrak{l})_l$, $\mathfrak{l}$ (not in $\mathfrak{p}_1$) being a left ideal in S. As a corollary of our theorem we obtain a necessary and sufficient condition for R to have a proper prime ideal. This condition enables us to get a view of all proper prime ideals of R. We shall also give a necessary and sufficient condition for (0) to be a prime ideal in R.

[4] Cf. e. g. B. L. VAN DER WAEREEN, loc. cit. [3], § 82.

[5] M. NAGATA calls an ideal *semi-prime* if it is the intersection of prime ideals. For this striking theorem, which it is evidently sufficient to prove for the case of prime ideals, we shall give in lemma 1 a proof based immediately on the definition. L. RÉDEI [3] proves a general theorem concerning this problem.

In § 3 we prove analogous results for the case when $\mathfrak{p}_1$ is a *complete* prime ideal in S.

Finally, in § 4 we apply our results to the Schreier extension of rings.

§ 2. Results on prime ideals

THEOREM 1. *Let* $\mathfrak{a}$ ($\neq (0), R$) *be an ideal in the ring* R, *and* $\mathfrak{p}$ *a prime ideal in* $\mathfrak{a}$.[6] *Then the ideal-quotient* $\mathfrak{p}_\mathfrak{a} = \mathfrak{p} : \mathfrak{a}$ *is a prime ideal in* R, *and*

$$\mathfrak{p}_\mathfrak{a} \cap \mathfrak{a} = \mathfrak{p}. \tag{4}$$

If $\mathfrak{p} \neq \mathfrak{a}$, *then* $\mathfrak{p}_\mathfrak{a}$ *is the only prime ideal in* R *whose intersection with* $\mathfrak{a}$ *is equal to* $\mathfrak{p}$. *In this case* $\mathfrak{p}_\mathfrak{a}$ *can be given also in the following four ways:*

$$\mathfrak{p}_\mathfrak{a} = (\mathfrak{p} : \mathfrak{a})_l = (\mathfrak{p} : \mathfrak{a})_r = (\mathfrak{p} : \mathfrak{l})_l = (\mathfrak{p} : \mathfrak{r})_r, \text{[7]} \tag{5}$$

where $\mathfrak{l}, \mathfrak{r}$ *are arbitrary left and right ideals in* $\mathfrak{a}$ *subject to the conditions* $\mathfrak{l}, \mathfrak{r}$ not in $\mathfrak{p}$.[8]

REMARK 1. By the second isomorphism theorem[9] theorem 1 implies that the ideal $(\mathfrak{a} + \mathfrak{p}_\mathfrak{a})/\mathfrak{p}_\mathfrak{a}$ of the factor-ring $R/\mathfrak{p}_\mathfrak{a}$ is isomorphic to the factor-ring $\mathfrak{a}/\mathfrak{p}$.

REMARK 2. The converse of a part of the above result is also true (cf. NAGATA [2], Theorem 9 a): A left ideal $\mathfrak{b}$ of R is a prime ideal in $\mathfrak{a}$ if and only if

$$\mathfrak{b}_\mathfrak{a} = \mathfrak{b} : \mathfrak{a} \tag{6}$$

is a prime ideal in R such that

$$\mathfrak{b} = \mathfrak{b}_\mathfrak{a} \cap \mathfrak{a}. \tag{7}$$

REMARK 3. (Cf. Remark 1 of NAGATA [2].) If $\mathfrak{p}$ is a prime ideal in the ideal $\mathfrak{a}$ and $\mathfrak{r}$ is a one-sided ideal in R satisfying $\mathfrak{r} \cap \mathfrak{a} = \mathfrak{p}$, then we have $\mathfrak{r} \subseteq \mathfrak{p}_\mathfrak{a}$.

REMARK 4. A prime ideal $\mathfrak{p}(\neq \mathfrak{a})$ of the ideal $\mathfrak{a}$ is a prime ideal in R if and only if $\mathfrak{p} = \mathfrak{p}_\mathfrak{a}$.

We have also the following

COROLLARY 1. Consider an arbitrary ideal $\mathfrak{a}(\neq (0))$ of the ring R. R contains a proper prime ideal if and only if either $\mathfrak{a}$ or $R/\mathfrak{a}$ contains a proper prime ideal.

[6] By ideal of the ideal $\mathfrak{a}$ of R we understand an ideal of $\mathfrak{a}$ considered as a ring.

[7] It is easily shown that the ideal-quotient $(\mathfrak{p} : \mathfrak{l})_l$ is identical with the maximal ideal $\mathfrak{m}$ in R, for which we have $\mathfrak{m}\mathfrak{l} \subseteq \mathfrak{p}$. A similar statement is true for the ideal-quotient $(\mathfrak{p} : \mathfrak{r})_r$.

[8] Such a left ideal in $\mathfrak{a}$ is for example $\mathfrak{a}\alpha(\alpha \in \mathfrak{a}, \notin \mathfrak{p})$. Indeed, $\mathfrak{p}$ being a prime ideal in $\mathfrak{a}$, if for the element $\alpha(\in \mathfrak{a})$ $\mathfrak{a}\alpha \subseteq \mathfrak{p}$, we have $\alpha \in \mathfrak{p}$. Similarly, for the right ideal $\alpha\mathfrak{a}$ in $\mathfrak{a}(\alpha \in \mathfrak{a}, \notin \mathfrak{p})$ we have $\alpha\mathfrak{a} \subseteq \mathfrak{p}$. We shall make use of these facts in the proof of corollary 2.

[9] For the first and second isomorphism theorems see N. BOURBAKI, *Algèbre* (Paris, 1951), Chap. I, pp. 130—131.

REMARK 5. Given an ideal $\mathfrak{a}(\neq(0))$ of R, all proper prime ideals of R can be obtained in the following way: First we form the ideal-quotients $\mathfrak{p}:\mathfrak{a}=\mathfrak{p}_{\mathfrak{a}}$ for all proper prime ideals $\mathfrak{p}$ of $\mathfrak{a}$. So we get all proper prime ideals of R not containing $\mathfrak{a}$. Then we consider the proper prime ideals of the factor-ring $R/\mathfrak{a}$ as sets of elements in R; so we obtain all proper prime ideals containing $\mathfrak{a}$.

In the proof of theorem 1 we shall make use of the following lemmas.

LEMMA 1. (Cf. NAGATA, Remark II.) If S is a left (right) ideal in the ring R, then every *proper* prime ideal (and so every proper complete prime ideal) $\mathfrak{p}$ of S is a right (left) ideal in R. If S is an ideal in R, then the prime ideals (complete prime ideals) of S are ideals in R too.[10]

PROOF. It suffices to prove the statement concerning, say, left ideals. Let S be a left ideal in R and $\mathfrak{p}(\neq S)$ a prime ideal in S. Let $\varkappa$ denote an element of $\mathfrak{p}$, σ an element of S not contained in $\mathfrak{p}$, and ϱ an arbitrary element of R. As we have $\varkappa\varrho S\sigma\subseteq\mathfrak{p}$, the prime property of $\mathfrak{p}$ in S and $\sigma\notin\mathfrak{p}$ imply $\varkappa\varrho\in\mathfrak{p}$, i. e. $\mathfrak{p}$ is a right ideal in R. It can be proved in the same way that in case S is a right ideal, $\mathfrak{p}$ is a left ideal in R.

LEMMA 2. (MCCOY.) If $\mathfrak{p}$ is a prime ideal in the ring R, then, for any ideal $\mathfrak{a}$ of R, $\mathfrak{a}\cap\mathfrak{p}$ is a prime ideal in $\mathfrak{a}$. (See MCCOY [1], Lemma 2.)

LEMMA 3. Let $\mathfrak{a}(\neq(0),R)$ be an ideal in the ring R and $\mathfrak{p}(\neq\mathfrak{a})$ a prime ideal in $\mathfrak{a}$. Let $\mathfrak{l}$ denote an arbitrary ideal in $\mathfrak{a}$ ($\mathfrak{l}$ not in $\mathfrak{p}$). If an ideal $\mathfrak{b}$ of R satisfies

(8) $$\mathfrak{b}\mathfrak{l}\subseteq\mathfrak{p}\quad\text{or}\quad\mathfrak{l}\mathfrak{b}\subseteq\mathfrak{p}\qquad(\mathfrak{l}\text{ not in }\mathfrak{p}),$$

it satisfies also

$$\mathfrak{b}\mathfrak{m}\subseteq\mathfrak{p}\quad\text{and}\quad\mathfrak{m}\mathfrak{b}\subseteq\mathfrak{p}$$

for any ideal $\mathfrak{m}$ of $\mathfrak{a}$.

PROOF. It is enough to prove the statement under the hypothesis of condition (8_1). For an arbitrary ideal $\mathfrak{m}$ of $\mathfrak{a}$, from (8_1) we obtain $\mathfrak{m}\mathfrak{b}\mathfrak{l}\subset\mathfrak{p}$. As $\mathfrak{m}\mathfrak{b}$ and $\mathfrak{l}$ are ideals in $\mathfrak{a}$ and $\mathfrak{l}$ not in $\mathfrak{p}$, owing to the definition of $\mathfrak{p}$ we have $\mathfrak{m}\mathfrak{b}\subseteq\mathfrak{p}$. Therefore, in particular,

(9) $$\mathfrak{l}\mathfrak{b}\subseteq\mathfrak{p}\qquad(\mathfrak{l}\text{ not in }\mathfrak{p})$$

is fulfilled. From (9) we obtain $\mathfrak{l}\mathfrak{b}\mathfrak{m}\subseteq\mathfrak{p}$, and hence $\mathfrak{b}\mathfrak{m}\subseteq\mathfrak{p}$ follows as before.

LEMMA 4. Let $\mathfrak{a}$ be an ideal in the ring R and $\mathfrak{p}$ a proper prime ideal in $\mathfrak{a}$. Let α denote an arbitrary element of $\mathfrak{a}$ not contained in $\mathfrak{p}$. If some element $\varrho(\in R)$ satisfies

(10) $$\varrho\mathfrak{a}\alpha\subseteq\mathfrak{p}\qquad(\alpha\in\mathfrak{a},\ \notin\mathfrak{p}),$$

then we have also $\varrho\mathfrak{a}\subseteq\mathfrak{p}$ and $\mathfrak{a}\varrho\subseteq\mathfrak{p}$.

[10] It is remarkable that whilst the proper prime ideals of the left ideal S are right ideals in R, the improper prime ideal $(=S)$ of S is a left ideal in R.

PROOF. For any element $\xi(\in \mathfrak{a})$, (10) implies $\xi\varrho\mathfrak{a}\alpha \subseteqq \mathfrak{p}$. As we have $\xi\varrho \in \mathfrak{a}, \alpha \in \mathfrak{a}$ and $\alpha \notin \mathfrak{p}$, from definition *b*) it follows $\xi\varrho \in \mathfrak{p}$, i. e. $\mathfrak{a}\varrho \subseteqq \mathfrak{p}$. So we have a fortiori

$$\alpha\mathfrak{a}\varrho \subseteqq \mathfrak{p} \qquad (\alpha \in \mathfrak{a}, \notin \mathfrak{p}), \tag{10'}$$

and hence $\varrho\mathfrak{a} \subseteqq \mathfrak{p}$ follows by the same arguments as before.

PROOF OF THEOREM 1. Let $\mathfrak{p}$ satisfy the conditions of the theorem. Then by lemma 1, $\mathfrak{p}$ is an ideal in R, so we can form the ideal-quotients (5).

It is obvious that in case $\mathfrak{a} = \mathfrak{p}$, $\mathfrak{a}_\mathfrak{a} = R$ is a prime ideal in R and (4) also holds. Therefore we may restrict ourselves to the case $\mathfrak{p} \neq \mathfrak{a}$. We show that the left ideal-quotient $(\mathfrak{p}:\mathfrak{a})_l$ is a prime ideal in R. As $\mathfrak{a}$ is an ideal in R, $(\mathfrak{p}:\mathfrak{a})_l$ is evidently also an ideal in R (see [1]). In order to show that it is a prime ideal, let $\mathfrak{m}, \mathfrak{n}$ be ideals in R satisfying $\mathfrak{m}\mathfrak{n} \subseteqq (\mathfrak{p}:\mathfrak{a})_l$. By the definition of $(\mathfrak{p}:\mathfrak{a})_l$,

$$\mathfrak{m}\cdot\mathfrak{n}\mathfrak{a} = \mathfrak{m}\mathfrak{n}\cdot\mathfrak{a} \subseteqq \mathfrak{p}. \tag{11}$$

If $\mathfrak{n}\mathfrak{a} \subseteqq \mathfrak{p}$, we have $\mathfrak{n} \subseteqq (\mathfrak{p}:\mathfrak{a})_l$. If $\mathfrak{n}\mathfrak{a}$ not in $\mathfrak{p}$, then, $\mathfrak{n}\mathfrak{a}$ being an ideal in $\mathfrak{a}$, (11) together with lemma 3 implies $\mathfrak{m}\mathfrak{a} \subseteqq \mathfrak{p}$; so we have $\mathfrak{m} \subseteqq (\mathfrak{p}:\mathfrak{a})_l$.

It can be shown in the same way that $(\mathfrak{p}:\mathfrak{a})_r$ is also a prime ideal in R.

Now we are going to prove

$$(\mathfrak{p}:\mathfrak{a})_l = (\mathfrak{p}:\mathfrak{a})_r. \tag{12}$$

If $\varrho \in (\mathfrak{p}:\mathfrak{a})_l$, we have $\varrho\mathfrak{a} \subseteqq \mathfrak{p}$. Hence we obtain the relation $\mathfrak{a}\varrho\mathfrak{a} \subseteqq \mathfrak{p}$. As $\mathfrak{a}$ not in $\mathfrak{p}$ and $\mathfrak{p}$ is a prime ideal in $\mathfrak{a}$, we have $\mathfrak{a}\varrho \subseteqq \mathfrak{p}$, i. e. $(\mathfrak{p}:\mathfrak{a})_l \subseteqq (\mathfrak{p}:\mathfrak{a})_r$. The inclusion relation $(\mathfrak{p}:\mathfrak{a})_r \subseteqq (\mathfrak{p}:\mathfrak{a})_l$ follows in a similar way, so we have proved (12). From (3) we get $\mathfrak{p}:\mathfrak{a} = (\mathfrak{p}:\mathfrak{a})_l = (\mathfrak{p}:\mathfrak{a})_r$, consequently, the ideal-quotient $\mathfrak{p}_\mathfrak{a} = \mathfrak{p}:\mathfrak{a}$ is a prime ideal in R.

Instead of (4), because of the equality $\mathfrak{p}_\mathfrak{a} = \mathfrak{p}:\mathfrak{a} = (\mathfrak{p}:\mathfrak{a})_l$ it is sufficient to prove

$$\mathfrak{p} = (\mathfrak{p}:\mathfrak{a})_l \cap \mathfrak{a}. \tag{4'}$$

For this purpose let $\sigma \in (\mathfrak{p}:\mathfrak{a})_l \cap \mathfrak{a}$; then we have

$$\sigma\mathfrak{a} \subseteqq \mathfrak{p} \qquad (\sigma \in \mathfrak{a}) \tag{13}$$

and $\mathfrak{p}$ being a prime ideal in $\mathfrak{a}$, $\sigma \in \mathfrak{p}$ follows readily.[11] Therefore $(\mathfrak{p}:\mathfrak{a})_l \cap \mathfrak{a} \subseteqq \mathfrak{p}$. Conversely, from $\mathfrak{p} \subseteqq \mathfrak{a}$, $\mathfrak{p} \subseteqq (\mathfrak{p}:\mathfrak{a})_l$ we conclude $\mathfrak{p} \subseteqq (\mathfrak{p}:\mathfrak{a})_l \cap \mathfrak{a}$, establishing (4′) (and (4)).

We show that if $\mathfrak{p} \neq \mathfrak{a}$, then $\mathfrak{p}:\mathfrak{a} = (\mathfrak{p}:\mathfrak{a})_l$ is the unique prime ideal in R whose intersection with $\mathfrak{a}$ is $\mathfrak{p}$. Suppose that $\mathfrak{o}$ is a prime ideal in R satisfying

$$\mathfrak{o} \cap \mathfrak{a} = \mathfrak{p} \qquad (\mathfrak{a} \neq \mathfrak{p}). \tag{14}$$

(14) implies $\mathfrak{o}\mathfrak{a} \subseteqq \mathfrak{p}$, and hence, by the definition of $(\mathfrak{p}:\mathfrak{a})_l$, we obtain $\mathfrak{o} \subseteqq (\mathfrak{p}:\mathfrak{a})_l$. Conversely, $(\mathfrak{p}:\mathfrak{a})_l\mathfrak{a} \subseteqq \mathfrak{p}$ implies $(\mathfrak{p}:\mathfrak{a})_l\mathfrak{a} \subseteqq \mathfrak{o}$, and thus, $\mathfrak{o}$ being a

11 Cf. e. g. NAGATA [2], lemma 1.

prime ideal in R such that $\mathfrak{a}$ not in $\mathfrak{o}$, we have $(\mathfrak{p}:\mathfrak{a})_l \subseteqq \mathfrak{o}$. Therefore $\mathfrak{o} = (\mathfrak{p}:\mathfrak{a})_l$ and our statement is proved.

It remains to prove the second part of (5). Let $\mathfrak{l}$ be a left ideal of $\mathfrak{a}$, not contained in $\mathfrak{p}$ (i. e. $\mathfrak{l}$ not in $\mathfrak{p}$). We are going to show only

(15) $$(\mathfrak{p}:\mathfrak{a})_l = (\mathfrak{p}:\mathfrak{l})_l.$$

$\varrho \in (\mathfrak{p}:\mathfrak{a})_l$ implies $\varrho\mathfrak{a} \subseteqq \mathfrak{p}$ and so a fortiori we have $\varrho\mathfrak{l} \subseteqq \mathfrak{p}$; therefore $(\mathfrak{p}:\mathfrak{a})_l \subseteqq \subseteqq (\mathfrak{p}:\mathfrak{l})_l$. Conversely, if $\sigma \in (\mathfrak{p}:\mathfrak{l})_l$, then we have $\sigma\mathfrak{l} \subseteqq \mathfrak{p}$. Hence we obtain the relation $\mathfrak{a}\sigma\cdot\mathfrak{l} = \mathfrak{a}\cdot\sigma\mathfrak{l} \subseteqq \mathfrak{p}$. Since $\mathfrak{a}\sigma$ and $\mathfrak{l}$ are left ideals in $\mathfrak{a}$, further $\mathfrak{l}$ not in $\mathfrak{p}$ and $\mathfrak{p}$ is a prime ideal, therefore we have $\mathfrak{a}\sigma \subseteqq \mathfrak{p}$, i. e. $(\mathfrak{p}:\mathfrak{l})_l \subseteqq (\mathfrak{p}:\mathfrak{a})_r$. However, $(\mathfrak{p}:\mathfrak{a})_l = (\mathfrak{p}:\mathfrak{a})_r$, thus we obtain $(\mathfrak{p}:\mathfrak{l})_l \subseteqq (\mathfrak{p}:\mathfrak{a})_l$, and so we have proved (15).

As the relation

(16) $$(\mathfrak{p}:\mathfrak{a})_r = (\mathfrak{p}:\mathfrak{r})_r$$

with any right ideal $\mathfrak{r}$ in $\mathfrak{a}$ ($\mathfrak{r}$ not in $\mathfrak{p}$) can be proved in an entirely analogous way, we have verified (5) and hence finished the proof of theorem 1.

Remark 1 does not need any proof.

Remark 2 can be proved in the following way: the necessity of conditions (6), (7) is stated in theorem 1. The sufficiency follows from lemma 2: as $\mathfrak{b}_\mathfrak{a}$ is a prime ideal in R, $\mathfrak{b}_\mathfrak{a} \cap \mathfrak{a} = \mathfrak{b}$ is a prime ideal in $\mathfrak{a}$.

The statement of remark 3 is obvious in case $\mathfrak{p} = \mathfrak{a}$, for then we have $\mathfrak{a}_\mathfrak{a} = R$. Therefore let $\mathfrak{p}$ be a prime ideal in $\mathfrak{a}$, and $\mathfrak{r}$ a right ideal in R such that $\mathfrak{r} \cap \mathfrak{a} = \mathfrak{p}$. Then $\mathfrak{r}\mathfrak{a} \subseteqq \mathfrak{p}$ and so by the definition of $(\mathfrak{p}:\mathfrak{a})_l$ we have $\mathfrak{r} \subseteqq (\mathfrak{p}:\mathfrak{a})_l$; therefore, by (5), $\mathfrak{r} \subseteqq \mathfrak{p}_\mathfrak{a}$. If $\mathfrak{r}$ is a left ideal in R, then we have in a similar manner our statement.

In remark 4, $\mathfrak{p}$ is evidently an ideal in R and $\mathfrak{a}$ not in $\mathfrak{p}$. If $\mathfrak{p} = \mathfrak{p}_\mathfrak{a}$, then $\mathfrak{p}$ is, by theorem 1, a prime ideal in R.

If, however $\mathfrak{p} \neq \mathfrak{p}_\mathfrak{a}$, then we have $\mathfrak{p}_\mathfrak{a}$ not in $\mathfrak{p}$ (since $\mathfrak{p} \subset \mathfrak{p}_\mathfrak{a}$). $\mathfrak{p}_\mathfrak{a}\mathfrak{a} \subseteqq \mathfrak{p}$ holds by the definition of $\mathfrak{p}_\mathfrak{a}$, but we have neither $\mathfrak{p}_\mathfrak{a} \subseteqq \mathfrak{p}$ nor $\mathfrak{a} \subseteqq \mathfrak{p}$. Consequently, $\mathfrak{p}$ is no prime ideal in R.

In order to prove corollary 1, let us consider an arbitrary ideal $\mathfrak{a}(\neq(0))$ in R. If $\mathfrak{o}$ is a proper prime ideal of R, then let $\mathfrak{p}$ denote the intersection of $\mathfrak{o}$ and $\mathfrak{a}$.

Case 1. If $\mathfrak{p} \subset \mathfrak{a}$, $\mathfrak{p}$ is a proper prime ideal in $\mathfrak{a}$ in view of lemma 2.

Case 2. If $\mathfrak{p} = \mathfrak{a}$, we have $\mathfrak{o} \supseteqq \mathfrak{a}$. Applying the first isomorphism theorem[9] we obtain

(17) $$R/\mathfrak{o} \simeq (R/\mathfrak{a})/(\mathfrak{o}/\mathfrak{a}).$$

So, if $\mathfrak{o}$ is a proper prime ideal in R, $\mathfrak{o}/\mathfrak{a}$ is a proper prime ideal in $R/\mathfrak{a}$.[12]

[12] This statement can be proved in the following way: Let $\bar{\varrho}$ ($\varrho \in R$) denote the residue-class $\varrho + \mathfrak{a}$ in $\bar{R} = R/\mathfrak{a}$, and let $\mathfrak{o}$ be a proper prime ideal in the ring R containing $\mathfrak{a}$. If $\bar{\varrho}\bar{R}\bar{\sigma} \subseteqq \mathfrak{o}/\mathfrak{a}$, then $\varrho R\sigma \subseteqq \mathfrak{o}$, and since $\mathfrak{o}$ is by assumption a prime ideal, we have either $\varrho \in \mathfrak{o}$ or $\sigma \in \mathfrak{o}$, so $\bar{\varrho} \in \mathfrak{o}/\mathfrak{a}$ or $\bar{\sigma} \in \mathfrak{o}/\mathfrak{a}$; $\mathfrak{o}/\mathfrak{a}$ is a prime ideal in $R/\mathfrak{a}$. As $\mathfrak{o}/\mathfrak{a} \neq R/\mathfrak{a}$ follows from $\mathfrak{o} \neq R$, $\mathfrak{o}/\mathfrak{a}$ is a proper prime ideal.

Conversely, if the ideal $\mathfrak{a}(\neq(0))$ has a proper prime ideal $\mathfrak{p}$, then by theorem 1, the ideal-quotient $\mathfrak{p}:\mathfrak{a}$ is a proper prime ideal in R. On the other hand, if the factor-ring $R/\mathfrak{a}$ contains a proper prime ideal $\mathfrak{o}/\mathfrak{a}=\{\mathfrak{a}, \varrho_1+\mathfrak{a}, \varrho_2+\mathfrak{a}, \ldots\}$, then the set of all elements in the residue classes belonging to $\mathfrak{o}/\mathfrak{a}$ is easily seen to be a proper prime ideal in R.[13] The proof of corollary 1 is thus finished.

In order to prove remark 5, we establish two classes of the proper prime ideals in R. The prime ideals containing $\mathfrak{a}$ form the class C_1, while the other prime ideals belong to class C_2. The prime ideals belonging to the class C_1 can be given by (17) as sets of elements in the residue classes of the proper prime ideals of $R/\mathfrak{a}$.

By theorem 1, the intersections of the prime ideals belonging to C_2 with $\mathfrak{a}$ are *different* prime ideals $\mathfrak{p}\subset\mathfrak{a}$. If we take *all* proper prime ideals $\mathfrak{p}$ of $\mathfrak{a}$, it follows from theorem 1 that the ideal-quotients $\mathfrak{p}_\mathfrak{a}$ exhaust all prime ideals of the class C_2.

In what follows we shall need the following definition. We call the ring R *almost zero-divisor free* if (0) is a prime ideal in it.[14] Accordingly, we shall call the ideal $\mathfrak{a}$ almost zero-divisor free if $\mathfrak{a}$ regarded as a ring is almost zero-divisor free. Evidently, the factor-ring $R/\mathfrak{o}$ is almost zero-divisor free if and only if $\mathfrak{o}$ is a prime ideal in R.

Corollary 2. The ring R is almost zero-divisor free if and only if at least one of the almost zero-divisor free ideals of R, say $\mathfrak{a}$, contains an element $\alpha(\neq 0)$ for which the equation

$$\beta\mathfrak{a}\alpha=(0) \qquad (0\neq\alpha\in\mathfrak{a};\ \beta\in R) \tag{18}$$

has the unique solution $\beta=0$.

Proof. First of all we know that $\mathfrak{a}\alpha, \alpha\mathfrak{a}$ $(\alpha\in\mathfrak{a}, \notin\mathfrak{p})$ are left (respectively right) ideals in $\mathfrak{a}$ for which $\mathfrak{a}\alpha, \alpha\mathfrak{a}$ not in $\mathfrak{p}$ (cf. [8]), therefore we have, by (5),

$$\mathfrak{p}_\mathfrak{a}=(\mathfrak{p}:\mathfrak{a})_l=(\mathfrak{p}:\mathfrak{a})_r=(\mathfrak{p}:\mathfrak{a}\alpha)_l=(\mathfrak{p}:\alpha\mathfrak{a})_r. \tag{5'}$$

The statement of corollary 2 follows immediately from remark 4, since because of $\mathfrak{p}=(0)$ and (5′), the fact that $\beta=0$ is the only solution of equation (18) is just the necessary and sufficient condition in remark 4.

Here we give also an other proof which makes use only of lemma 4. The condition is necessary, for if the equation (18) had a solution $\beta(\neq 0, \in R)$ for every element $\alpha(\neq 0, \in\mathfrak{a})$,[15] then lemma 4 would imply $\beta\mathfrak{a}=(0)$. As

[13] We obtain this statement applying the former inference in an inverse order.

[14] McCoy calls a ring with this property a prime ring. We prefer the above terminology, for every zero-divisor free ring is almost zero-divisor free; further, in an almost zero-divisor free ring R $\mathfrak{a}\mathfrak{b}=(0)$ (with $\mathfrak{a}$, $\mathfrak{b}$ ideals in R) implies $\mathfrak{a}=(0)$ or $\mathfrak{b}=(0)$; finally, if for the elements $\alpha, \beta(\in R)$ we have $\alpha R\beta=(0)$, then either $\alpha=0$ or $\beta=0$.

[15] If the equation (18) has a solution $\beta(\neq 0, \in R)$ for some element α, then by lemma 4 we have $\beta\mathfrak{a}\xi=(0)$, $\xi\mathfrak{a}\beta=(0)$ for *any* element $\xi(\in\mathfrak{a})$.

$\beta R\alpha \subseteq \beta\mathfrak{a} = (0)$ holds for each $\alpha(\neq 0, \in \mathfrak{a})$, and $\alpha \neq 0$, $\beta \neq 0$, therefore (0) is no prime ideal in R.

In order to prove the sufficiency of the condition, suppose that R is not almost zero-divisor free. Then by definition there exist elements $\varrho, \sigma(\neq 0)$ in R so that $\varrho R\sigma = (0)$. We show that in this case the equation (18) has a solution $\beta(\neq 0, \in R)$. The assumption implies $\varrho R\sigma\mathfrak{a}\alpha = (0)$ (where $\alpha \neq 0, \in \mathfrak{a}$). If $\sigma\mathfrak{a}\alpha = (0)$, the solution is $\beta = \sigma \neq 0$; if, however, $\sigma\mathfrak{a}\alpha \neq (0)$, then we have, for any non-zero element α' of $\sigma\mathfrak{a}\alpha$, $\varrho R\alpha' = (0)$ and a fortiori $\varrho\mathfrak{a}\alpha' = (0)$. Therefore, by lemma 4, we have $\varrho\mathfrak{a} = (0)$ and $\varrho\mathfrak{a}\alpha = (0)$ $(\alpha \neq 0, \in \mathfrak{a})$, so the corresponding solution is now $\beta = \varrho \neq 0$. Thereby we have proved corollary 2.

§ 3. Results on complete prime ideals

We have the following analogue of theorem 1:

THEOREM 1'. *Let $\mathfrak{a}(\neq (0), R)$ be an ideal in the ring R, and $\mathfrak{q}$ a complete prime ideal in $\mathfrak{a}$. Then the ideal-quotient $\mathfrak{q}_\mathfrak{a} = \mathfrak{q} : \mathfrak{a}$ is a complete prime ideal in R, and*

$$\mathfrak{q}_\mathfrak{a} \cap \mathfrak{a} = \mathfrak{q}. \tag{19}$$

If $\mathfrak{q} \neq \mathfrak{a}$, $\mathfrak{q}_\mathfrak{a}$ is the only complete prime ideal in R, the intersection of which with $\mathfrak{a}$ gives $\mathfrak{q}$. In that case $\mathfrak{q}_\mathfrak{a}$ can be given also in the following four ways:

$$\mathfrak{q}_\mathfrak{a} = (\mathfrak{q} : \mathfrak{a})_l = (\mathfrak{q} : \mathfrak{a})_r = (\mathfrak{q} : \alpha)_l = (\mathfrak{q} : \alpha)_r, \tag{20}$$

where α denotes an arbitrary element of $\mathfrak{a}$ not contained in $\mathfrak{q}$.

Remarks 1—5 and corollary 1 are true for complete prime ideals instead of prime ideals. The proofs can be carried out in an entirely analogous way, therefore we omit to formulate them.

We prove also the following lemmas:

LEMMA 2'. If $\mathfrak{q}$ is a complete prime ideal in R, for any subring S of R $\mathfrak{q} \cap S = \mathfrak{q}'$ is a complete prime ideal in S.

PROOF. It is obvious that $\mathfrak{q}'$ is an ideal in S. Suppose we have $\alpha\beta \in \mathfrak{q}'$; $\alpha, \beta \in S$. Then a fortiori $\alpha\beta \in \mathfrak{q}$. As $\mathfrak{q}$ is a complete prime ideal in R, we have α or $\beta \in \mathfrak{q}$, and so α or $\beta \in \mathfrak{q}'$.

LEMMA 4'. Let $\mathfrak{a}$ be an ideal in the ring R and $\mathfrak{q}$ a proper complete prime ideal in $\mathfrak{a}$. Let α denote an arbitrary element of $\mathfrak{a}$, not contained in $\mathfrak{q}$. If, some element $\beta(\in R)$ satisfies

$$\beta\alpha \in \mathfrak{q} \quad \text{or} \quad \alpha\beta \in \mathfrak{q} \qquad (\alpha \in \mathfrak{a}, \notin \mathfrak{q};\ \beta \in R), \tag{21}$$

then we have also $\beta\xi \in \mathfrak{q}$, $\xi\beta \in \mathfrak{q}$ for any element $\xi(\in \mathfrak{a})$. I. e. we have $(\mathfrak{q} : \alpha)_l$, $(\mathfrak{q} : \alpha)_r \subseteq (\mathfrak{q} : \mathfrak{a})_l$, $(\mathfrak{q} : \mathfrak{a})_r$.

PROOF. (21_1) implies $(\xi\beta)\alpha \in \mathfrak{q}$ for any $\xi(\in \mathfrak{a})$, so that $\mathfrak{q}$ is a complete prime ideal in $\mathfrak{a}$ and $\alpha \notin \mathfrak{q}$, we have $\xi\beta \in \mathfrak{q}$. In the special case $\xi = \alpha$ we have

$\alpha\beta \in \mathfrak{q}(\alpha \in \mathfrak{a}, \notin \mathfrak{q})$, whence $\beta\xi \in \mathfrak{q}$ follows as before. Starting from (21_2) the result can be obtained in the same way.

Proof of theorem 1′. By lemma 1, $\mathfrak{q}$ is an ideal in R, so we can form the ideal-quotients (20).

It is obvious that in case $\mathfrak{q} = \mathfrak{a}$, $\mathfrak{q}_\mathfrak{a} = R$ is a complete prime ideal in R and (19) is also satisfied.

In what follows we suppose $\mathfrak{q} \neq \mathfrak{a}$. As $(\mathfrak{q}:\mathfrak{a})_l \subseteq (\mathfrak{q}:\alpha)_l$ and $(\mathfrak{q}:\mathfrak{a})_r \subseteq (\mathfrak{q}:\alpha)_r$, the last statement of lemma 4′ implies

$$(20') \qquad (\mathfrak{q}:\mathfrak{a})_l = (\mathfrak{q}:\alpha)_l \quad \text{and} \quad (\mathfrak{q}:\mathfrak{a})_r = (\mathfrak{q}:\alpha)_r \qquad (\alpha \in \mathfrak{a}, \notin \mathfrak{q}).$$

From (20′) and the last statement of lemma 4′ we conclude $(\mathfrak{q}:\alpha)_l \subseteq ((\mathfrak{q}:\mathfrak{a})_r =)$ $(\mathfrak{q}:\alpha)_r$ and $(\mathfrak{q}:\alpha)_r \subseteq ((\mathfrak{q}:\mathfrak{a})_l =)$ $(\mathfrak{q}:\alpha)_l$; therefore we have

$$(20'') \qquad (\mathfrak{q}:\alpha)_l = (\mathfrak{q}:\alpha)_r \qquad (\alpha \in \mathfrak{a}, \notin \mathfrak{q})$$

which, together with (20′) proves (20).

In order to establish that $\mathfrak{q}_\mathfrak{a}$ is a complete prime ideal in R, by (20) it is sufficient to prove the same for $(\mathfrak{q}:\alpha)_l$. Therefore let $\varrho, \sigma \in R$ and $\varrho\sigma \in (\mathfrak{q}:\alpha)_l$, whence $\varrho\sigma\alpha \in \mathfrak{q}$. If $\sigma\alpha \in \mathfrak{q}$, we have $\sigma \in (\mathfrak{q}:\alpha)_l$. If $\sigma\alpha = \alpha'(\in \mathfrak{a})$ does not belong to $\mathfrak{q}$, from $\varrho\alpha' \in \mathfrak{q}$ we conclude, by lemma 4′, $\varrho\alpha \in \mathfrak{q}$; so we have now $\varrho \in (\mathfrak{q}:\alpha)_l$, i. e. $(\mathfrak{q}:\alpha)_l$, and therefore $\mathfrak{q}_\mathfrak{a}$ is a complete prime ideal in R, in fact.

(19) is only an application of (4) to the case when $\mathfrak{p} = \mathfrak{q}$ is a complete prime ideal.

Finally, we have to prove that $\mathfrak{q}_\mathfrak{a}$ is the only complete prime ideal in R whose intersection with $\mathfrak{a}$ is $\mathfrak{q}$. As every complete prime ideal is a prime ideal, this is a consequence of theorem 1.

So we have completely proved theorem 1′.

In the particular case $\mathfrak{q} = (0)$ we obtain as a corollary of theorem 1′ the results of my paper [4]; here we state only [4] theorem 2:

Corollary 2′. The ring R is zero-divisor free if and only if there exists a zero-divisor free ideal $\mathfrak{a}$ of R containing an element $\alpha(\neq 0)$ which is no left zero-divisor in R.

§ 4. Applications to the Schreier extension of rings

By a Schreier extension of the ring P by the ring R we mean a ring $\mathfrak{R}$ which contains an ideal P' such that

$$(22) \qquad \mathfrak{R}/\mathrm{P}' \cong R, \quad \mathrm{P}' \cong \mathrm{P}$$

are satisfied. Evidently, P can be identified with P', so that the results of the former sections can be applied to the ring $\mathfrak{R}$, the ideal P and the factor-ring $(\mathfrak{R}/\mathrm{P} \cong)R$. Here we limit ourselves to the formulation of some of the former results for the mentioned case.

THEOREM 2. *A Schreier extension $\mathfrak{R}$ of the ring P by the ring R contains a proper (complete) prime ideal if and only if either P or R contains a proper (complete) prime ideal.*

Further, all proper (complete) prime ideals of the ring $\mathfrak{R}$ can be determined by the aid of the proper (complete) prime ideals of P and R.[16]

THEOREM 3. *A Schreier extension $\mathfrak{R}$ of the ring P by R is almost zero-divisor free if and only if P is almost zero-divisor free and P contains an element $\alpha(\neq 0)$, for which the equation*

$$\beta \mathrm{P} \alpha = 0 \qquad (\beta \in \mathfrak{R};\ \alpha \neq 0,\ \in \mathrm{P})$$

has the unique solution $\beta = 0$.[17]

(Received 10 August 1953)

Bibliography

[1] N. H. McCoy, Prime ideals in general rings, *Amer. Journ. Math.*, **71** (1949), pp. 823—833.
[2] M. Nagata, On the theory of radicals in a ring, *Journ. Math. Soc. Japan*, **3** (1951), pp. 300—344.
[3] L. Rédei, Die Holomorphentheorie für Gruppen und Ringe, *Acta Math. Acad. Sci. Hung.*, **5** (1954) (under press).
[4] O. Steinfeld, Über die Nullteilerfreiheit von Ringen, *Publicationes Math. (Debrecen)*, **2** (1952), pp. 281—285.

[16] Here we do not point out the details.

[17] This theorem is analogous to Steinfeld [4], theorem 3; here we omit to formulate it in terms of the notions of the Schreier extension theory.

О ЧАСТНЫХ ИДЕАЛОВ И О ПРОСТЫХ ИДЕАЛАХ

О. ШТЕЙНФЕЛД (Сегед)

(Резюме)

Если $\mathfrak{b}$—идеал в кольце R, а H—некоторое подмножество от R, то мы называем их **частным** и обозначаем через $\mathfrak{b}:H$ множество тех элементов β, для которых

$$\beta H \subseteq \mathfrak{b} \quad \text{и} \quad H\beta \subseteq \mathfrak{b}.$$

Идеал $\mathfrak{p}$ в кольце R называется **простым**, если для двух идеалов $\mathfrak{a}$ и $\mathfrak{b}$ кольца R из $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p}$ следует, что или $\mathfrak{a} \subseteq \mathfrak{p}$ или $\mathfrak{b} \subseteq \mathfrak{p}$.

Развивая дальше результат японского математика М. Нагата, автор показывает следующее:

Если $\mathfrak{a}(\neq R)$ идеал в кольце R, а $\mathfrak{p}$—простой идеал в $\mathfrak{a}$, то частное $\mathfrak{p}:\mathfrak{a}$ является единственным простым идеалом в R, пересечение которого с $\mathfrak{a}$ равно $\mathfrak{p}$ и если $\mathfrak{q}$—односторонний идеал в R, для которого $\mathfrak{q} \cap \mathfrak{a} = \mathfrak{p}$, то $\mathfrak{q} \subseteq \mathfrak{p}:\mathfrak{a}$.

На основе этой теоремы получается хороший обзор простых идеалов кольца R. Можно далее задать простое необходимое и достаточное условие для того, чтобы (0) был простым идеалом в R.

Совершенно аналогичные результаты получаются в случае, когда $\mathfrak{p}$ вполне простой идеал в $\mathfrak{a}$. (Вполне простым мы называем идеал $\mathfrak{p}$ кольца R, если из $\alpha\beta \in \mathfrak{p}\ (\alpha, \beta \in R)$ следует, что либо $\alpha \in \mathfrak{p}$, либо $\beta \in \mathfrak{p}$.)

Все эти результаты применимы к расширению $\mathfrak{R}$ кольца P с помощью кольца R.

ON A SPECIAL KIND OF DUALITY IN GROUP THEORY. II

By
L. FUCHS (Budapest)
(*Presented by* L. RÉDEI)

§ 1. Introduction

In a recent note[1] T. SZELE, A. KERTÉSZ and the present author have considered several problems arisen in connection with a special kind of duality in group theory and solved them for the case of countable abelian groups. The present paper is devoted to extending these results to abelian groups of arbitrary power.

After laying down the notations and terminologies used throughout the discussions, we shall prove some preliminary lemmas which we shall need several times. Some of these lemmas have also certain own interest, since they state the possibility of a direct decomposition of the group G where the powers of the components are some cardinal numbers depending on G. Then we proceed to consider the problem of determining all pairs of $F—S$-dual groups, firstly for the case of p-groups (and hence for torsion groups), and secondly for mixed groups (§ 4 resp. § 5). Finally, in § 6 we characterize all pairs of dual groups and all selfdual groups. It will turn out that a surprisingly great role is played by arguments of partly set-theoretic character and in the descriptions of the groups in question one has to use throughout cardinal numbers.

We remark that there is, however, a certain gap in our results which lies in the fact that we did not succeed in giving an explicit form for the p-groups containing no elements of infinite height and having Property $A_{\mathfrak{p}}$ (see § 2). In the case of countable groups PRÜFER's famous theorem[2] settles this problem, the condition being unboundedness (for $\mathfrak{p} \leqq \aleph_0$), but the general case seems to be rather difficult.[2a]

1 See [5]. Numbers in brackets refer to the Bibliography given at the end of this paper.

2 PRÜFER [10]: A countable abelian p-group without elements of infinite height is the direct sum of cyclic groups.

2a *(Added in proof, 25 December 1953.)* In the meantime T. SZELE has proved that a p-group has Property $A_{\mathfrak{p}}$ if and only if the same is true for its basic subgroup. Since the basic subgroup is the direct sum of cyclic groups and for such groups it is quite obvious when they have Property $A_{\mathfrak{p}}$, this result fills out the gap of the present paper.

§ 2. Notation and terminology

By a group we shall mean throughout an additive abelian group with more than one element. Groups will be denoted by Latin capital letters, their elements by a, g, h, x, while i, j, k, m, n will mean as usual rational integers, in particular p a prime and $p_1, p_2, \dots$ the sequence of all natural primes. Small Gothic types such as $\mathfrak{p}, \mathfrak{q}, \mathfrak{r}, \mathfrak{s}, \mathfrak{t}$ denote cardinal numbers.

By $O(a)$ we denote the order of a group element a. For a subset S of a group G, $\{S\}$ and $|S|$ will denote the subgroup generated by S resp. the power of S. The sign "$+$" is used to denote (besides group operation) direct sum and for a cardinal number $\mathfrak{p}$, $\sum_{\mathfrak{p}} C$ means the (discrete) direct sum of $\mathfrak{p}$ groups, each isomorphic to a given group C.

The cyclic group of order r will be denoted by $\mathfrak{Z}(r)$ for $1 \leqq r \leqq \infty$, while $\mathfrak{Z}(p^\infty)$ serves to denote the quasicyclic group (or group of type p^∞) and $\mathfrak{R}$ the additive group of all rational numbers. It is known that each complete (or algebraically closed[3]) abelian group G (defined so as to satisfy $nG = G$ for all non-zero integers n) is the direct sum of groups $\mathfrak{Z}(p^\infty)$ and $\mathfrak{R}$, and is a direct summand of every group containing it.[4] H is called a serving subgroup of G if for each $a \in H$, the solvability of $nx = a$ in G implies its solvability in H. B is termed a basic subgroup[5] of the p-group G if B is the direct sum of cyclic groups, is a serving subgroup of G and the factorgroup G/B is complete.

If G is a p-group then an element a in G is said to have the height k if k is the greatest non-negative integer for which $p^k x = a$ is solvable in G. In case there is no maximal k of this property, then a is of infinite height. The zero element may be considered both as of finite and infinite height. In a p-group G all elements of infinite height form a subgroup G^* and the factorgroup G/G^* is called the first Ulm factor[6] of G.

A subset $S = (a_\nu)$ of G, not containing 0, is said to be independent if for any finite subset $a_1, \dots, a_k$ of S a relation

$$n_1 a_1 + \cdots + n_k a_k = 0 \qquad (n_i \text{ rational integers})$$

implies $n_1 a_1 = \cdots = n_k a_k = 0$, i. e. $n_i = 0$ in case $O(a_i) = \infty$ and $O(a_i) | n_i$ in case $O(a_i)$ is finite. By the rank $\mathfrak{R}(G)$ of G we understand the cardinal number of a maximal independent system in G containing but elements of infinite or prime-power order; $\mathfrak{R}(G)$ is an invariant of G and it is easy to see that $\mathfrak{R}(G) = |G|$ provided $\mathfrak{R}(G) \geqq \aleph_0$. By the torsion free rank $\mathfrak{R}_\infty(G)$ resp. by the p_i-rank $\mathfrak{R}_{p_i}(G)$ of G we mean the power of a maximal inde-

[3] Szele [11].
[4] Baer [1].
[5] This notion is due to Kulikov [7].
[6] Ulm [13] or Kurosh [9], p. 171.

pendent system containing but elements of infinite order resp. of order p_i^k $(k = 1, 2, \ldots)$.

For a p-group G, $\mathfrak{R}_{p^\infty}(G)$ will denote $\min\limits_{k=0,1,\ldots} \mathfrak{R}(p^k G)$ and if $\mathfrak{R}(G) \geqq \geqq \mathfrak{R}(pG) \geqq \cdots \geqq \mathfrak{R}(p^{m-1}G) > \mathfrak{R}(p^m G) = \mathfrak{R}_{p^\infty}(G)$, then the set $\mathfrak{R}(G)$, $\mathfrak{R}(pG), \ldots, \mathfrak{R}(p^m G)$ is called the set of invariants of G. In case $\mathfrak{R}_{p^\infty}(G) = = \mathfrak{R}(G)$, i. e. G has only one invariant, we shall call G *regular*. If G is an arbitrary torsion group or a mixed group and G_i denotes the p_i-component of G resp. that of the torsion subgroup of G, then we define $\mathfrak{R}_{p_i}(G) = \mathfrak{R}(G_i)$, or more generally, $\mathfrak{R}_{p_i}(p_i^k G) = \mathfrak{R}(p_i^k G_i)$, and call the totality of the invariants of the p_i-components G_i taken for all primes p_i, together with $\mathfrak{R}_\infty(G)$, the *invariants* of G.

As in [5], we denote by $S(G)$ and $F(G)$ the set of all subgroups and the set of all factorgroups of G, respectively. Recall that we have called the groups G and H *F—S-dual* if $F(G) = S(H)$, *S—F-dual* if $S(G) = F(H)$, *dual* if they are both F—S-dual and S—F-dual, further, the group G is said to be *selfdual* if $S(G) = F(G)$.

Finally, we introduce a terminology. We shall say that a p-group G *has Property* $A_\mathfrak{p}$ if it can be mapped homomorphically onto a group $A_\mathfrak{p}$ with

$$A_\mathfrak{p} = A_\mathfrak{p}(p) = \sum_{\mathfrak{p}} \sum_{k=1}^{\infty} \mathfrak{Z}(p^k), \tag{1}$$

i. e. onto the direct sum of $\mathfrak{p}$ groups, each isomorphic to the direct sum of cyclic groups of order $p, p^2, \ldots$, respectively. Considering that a homomorphic image of an element of infinite height is again an element of this property, it follows at once that a p-group G has Property $A_\mathfrak{p}$ if and only if its first Ulm factor possesses the same property. Hence we conclude that the problem of describing all p-groups with Property $A_\mathfrak{p}$ is equivalent to that of describing all p-groups without elements of infinite height having the same property. However, we did not succeed in getting a simple characterization of the latter type of group. We merely mention that if G is countable and $\mathfrak{p} \leqq \aleph_0$, then PRÜFER's fundamental theorem implies that the sought necessary and sufficient condition is unboundedness. (See footnote [2a].)

It is clear that *each p-group of power $\leqq \mathfrak{p}$ is a homomorphic image of* $A_\mathfrak{p}$. This is the reason why this type of group plays an important role in our investigations. Therefore $A_\mathfrak{p}$ is, in a certain respect, the dual notion of the algebraically closed p-group of power $\mathfrak{p}$, $\sum\limits_{\mathfrak{p}} \mathfrak{Z}(p^\infty)$ (each p-group of power $\leqq \mathfrak{p}$ is a subgroup of the last group).

§ 3. Preliminary lemmas

We shall several times make use of the following lemmas.

LEMMA 1. *If for a p-group G we have* $\mathfrak{R}_{p^\infty}(G) < \mathfrak{R}(G)$, *i. e. G is not regular, then G has a direct decomposition*

$$G = G_1 + G_2 \tag{2}$$

where G_1 *is a bounded group and* G_2 *is a regular group such that* $\mathfrak{R}(G_2) = \mathfrak{R}_{p^\infty}(G)$.

Let m be the least integer with $\mathfrak{R}(p^m G) = \mathfrak{R}_{p^\infty}(G) = \mathfrak{p}$. Using ZORN's lemma, we may construct a maximal serving[7] subgroup G_1 of G having the property $p^m G_1 = 0$. Then, by a well-known theorem,[8] we get a direct decomposition (2) for G. Here the rank of G_2 is not less than $\mathfrak{p}$, for $p^m G_2 = p^m G$, but it can neither exceed $\mathfrak{p}$. This latter statement follows immediately if one takes into account the known fact[9] that an element of order p and of finite height n may be imbedded in a cyclic direct summand of the group (the order of this summand is p^{n+1}), and that in a maximal independent system of G, consisting only of elements of order p, the power of the set of elements of height $\geqq m$ is evidently $\mathfrak{p}$. This establishes our assertion. (Observe that we have in addition proved that by construction G_2 contains no elements of order p and of height $\leqq m-1$.)

LEMMA 2. *Suppose the group G contains a torsion group H with the property that each infinite serving subgroup of H is contained in a direct summand of H having the same power.*[10] *Let* $F = G/H$. *Then G has a decomposition* $G = G_1 + G_2$ *where* G_1 *is a subgroup of H and* G_2 *satisfies*[11]

$$\mathfrak{R}_{p_i}(G_2) \leqq \max\left(\mathfrak{R}_{p_i}(F), \mathfrak{R}_\infty(F), \aleph_0\right). \tag{3}$$

Before entering into the proof we remark[12] that, *given any infinite subgroup K of an arbitrary torsion group H, there exists a serving subgroup of the same power* $|K|$ *containing K.* Obviously, it suffices to prove this statement only for p-groups. If K is an infinite subgroup of the p-group H

[7] Observe that the property of being a serving subgroup is of inductive character.

[8] KULIKOV [6]: If in a p-group G, H is a serving subgroup and is bounded (i. e. the orders of its elements are bounded), then H is a direct summand of G.

[9] KULIKOV [7], PRÜFER [10] and KUROSH [9], p. 164.

[10] It would be an interesting problem to characterize all groups with this property. That there are p-groups not possessing this property may be shown by the instance of the torsion subgroup of the complete direct sum of the cyclic groups of order $p, p^2, \ldots,$ respectively. The discrete direct sum of the same cyclic groups is a basic (and hence a serving) subgroup of this group, but can not be imbedded in a countable direct summand.

[11] If the p_i-rank of F is infinite and not less than its torsion free rank, then equation holds.

[12] This remark is due to SZELE [12].

and K is not yet serving, then in case the height k_a of $a \in K$ (taken in H) is finite, we determine an element x_a in H with $p^{k_a} x_a = a$, while if the height k_a is infinite then we determine countably many elements $x_a^{(n)}$ $(n = 1, 2, \ldots)$ such that $p^n x_a^{(n)} = a$. The elements x_a resp. $x_a^{(n)}$, taken for all a in K, generate a subgroup K_1 of H containing K. Doing the same with K_1 in place of K, we get a larger subgroup K_2 and for K_2 we repeat this construction etc. The union of all subgroups $K, K_1, K_2, \ldots$ is a subgroup of H which is clearly serving in H and has the same power as K. Therefore, if to each infinite serving subgroup S of H there exists a direct summand of H containing S and having the same power as S itself, then the same must be true for any subgroup of H whether it is serving or not.

After this introductory remark let us take a generating system $(\bar{a}_\nu)$ of F consisting of cosets modulo H whose order is either infinity or a power of a prime. (Clearly, there is no restriction in supposing that the set of $\bar{a}_\nu$ of infinite order is not greater than $\max(\mathfrak{R}_\infty(F), \aleph_0)$.) From each coset $\bar{a}_\nu$ we select an element a_ν of a possibly least order. Then the order of a_ν is again either infinity or a power of the same prime. Indeed, if $O(a_\nu)$ mod H is equal to p^s and we had $O(a_\nu) = p^t n$ with $t \geqq s, n > 1$ and $(n, p) = 1$, then by solving the equation $nu + p^t v = 1$ for rational integers u, v, we would get

$$a_\nu = nua_\nu + p^t va_\nu = a'_\nu + a''_\nu \quad \text{with} \quad a''_\nu \in H, O(a'_\nu) = p^t < O(a_\nu),$$

in contradiction to the choice of a_ν.

Now, let us put $G' = \{a_1, \ldots, a_\nu, \ldots\}$, $M = H \cap G'$, and denote by N the direct summand of H containing M and having the power $|M|$ (if M is finite then $|N| \leqq \aleph_0$). Then we have $H = G_1 + N$ for some subgroup G_1 of H and by putting $G_2 = \{G', N\}$ we obtain $G = G_1 + G_2$ as an immediate consequence of the representations $g = n_1 a_1 + n_2 a_2 + \cdots + n_k a_k + h$ (g arbitrary in $G, h \in H$) and $h = h_1 + h_2$ $(h_1 \in G_1, h_2 \in N)$ as well as of the fact that $G_1 \cap G_2 = 0$. We have still to verify the statement concerning G_2. In order to do this, observe that, by our preceding remark on $O(a_\nu)$, the p_i-component of G', and thus also that of M, has a power $\leqq \max(\mathfrak{R}_{p_i}(F), \mathfrak{R}_\infty(F), \aleph_0)$. The same must be true, of course, for N and hence for G_2. Thus the proof of Lemma 2 is completed.

The latter lemma has an interesting consequence in the theory of infinite abelian mixed groups. It is well known that in this theory an important problem is to get criteria under which the torsion subgroup T of a mixed group G is a direct summand. A theorem due to S. Fomin[13] states that this is the case if $nT = 0$ holds for some natural integer n (simple counter-examples show that this condition can not be weakened). Now, the following problem arises: By weakening the condition $nT = 0$ in a suitable manner, whether may one obtain a result stating that, though not the whole torsion

[13] See Fomin [2].

subgroup T, but at least a "good portion" of it is a direct summand of the whole group? This question may be answered by the following

COROLLARY. *Suppose the torsion subgroup T of G is of the property that each infinite serving subgroup of H belongs to a direct summand of T having the same power. Then G has a decomposition $G = G_1 + G_2$ where G_1 is a torsion group and* $|G_2| \leq \max(\mathfrak{R}_\infty(G), \aleph_0)$.

In fact, our assertion follows at once from Lemma 2, for now we have $\mathfrak{R}_\infty(G\,T) = \mathfrak{R}_\infty(G)$ and $\mathfrak{R}_{p_i}(G\,T) = 0$.

Combining Lemmas 1 and 2 we are led to the following result.

LEMMA 3. *Each mixed abelian group G has a decomposition $G = G_1 + G_2$ where G_1 is a torsion group whose p_i-components are bounded and G_2 is a mixed group such that*

$$\mathfrak{R}_{p_i}(G_2) \leq \max(\mathfrak{R}_{p_i^\infty}(G), \mathfrak{R}_\infty(G), \aleph_0). \tag{4}$$

For each prime p_i, we take a direct decomposition (2) of the p_i-component T_i of the torsion subgroup T of G and then choose for H the direct sum of the bounded direct summands of all T_i. In this case H is the direct sum of cyclic groups and thus possesses the property required in Lemma 2. (3) implies that (4) holds, indeed.

We also mention an important property of p-groups which will play an essential role in our discussions.

LEMMA 4. *Each abelian p-group G contains a basic subgroup B such that* $\mathfrak{R}(G/B) = \mathfrak{R}_{p^\infty}(G)$.

For the proof we refer to KULIKOV [8], Theorem 4.24, or FUCHS [4], p. 275.

A well-known theorem[14] states that any abelian group may be isomorphically imbedded in a complete group which is uniquely determined (up to an isomorphism) if minimality is assumed. A partly less and partly more statement is enunciated in

LEMMA 5. *If G is an abelian group with $\aleph_0 \leq \mathfrak{R}_\infty(G) = \mathfrak{r} \leq \mathfrak{R}_{p_i}(G) = \mathfrak{p}_i$ for each i, then G is isomorphic to some subgroup of the complete group*

$$C = \sum_{\mathfrak{r}} \mathfrak{R} + \sum_i \sum_{\mathfrak{p}_i} \mathfrak{Z}(p_i^\infty).$$

Proof on the same line as KULIKOV's elegant proof. G is clearly a homomorphic image of the group

$$D = \sum_{\mathfrak{r}} \mathfrak{Z}(\infty) + \sum_i A_{\mathfrak{p}_i}(p_i),$$

say,

$$G \simeq D/Z.$$

If we imbed D in C in the obvious manner, then we see that $C\,Z$ as a

[14] KULIKOV [7], KUROSH [9], p. 151 and SZELE [11].

factorgroup of the complete group C is itself a complete group and the hypothesis $\mathfrak{p}_i \geqq \mathfrak{r}$ ensures that C/Z can be imbedded in C, thus finishing the proof.

§ 4. *F—S*-dual *p*-groups

A complete characterization of all pairs of F—S-dual (and hence S—F-dual) p-groups is contained in the following theorem.

THEOREM 1. *Let G be an abelian p-group with $\mathfrak{R}(G) = \mathfrak{q}$ and $\mathfrak{R}_{p^\infty}(G) = \mathfrak{p}$. The p-groups G and H are F—S-dual if and only if they are of the form*

(5) $$G = G_1 + G_2 + G_3 \quad \text{and} \quad H = H_1 + H_2 + H_3$$

where

(i) *in case $\mathfrak{p} = \mathfrak{q}$: $G_1 = H_1 = 0$;*
in case $\mathfrak{p} < \mathfrak{q}$: $p^m G_1 = p^m H_1 = 0$ for some natural integer m such that $\mathfrak{R}(G_1) = \mathfrak{R}(H_1) = \mathfrak{q}$ and $\mathfrak{R}(p^k G_1) = \mathfrak{R}(p^k H_1)$ $(k = 0, 1, \ldots)$ (thus G_1 and H_1 are direct sums of cyclic groups of bounded order);

(ii) $G_2 = \sum\limits_{\mathfrak{s}} \mathfrak{Z}(p^\infty)$ *with* $0 \leqq \mathfrak{s} \leqq \mathfrak{p}$;

(iii) *G_3 is a reduced and regular p-group of power $\mathfrak{p}$ whose first Ulm factor has Property $A_\mathfrak{p}$;*

(iv) $H_2 = \sum\limits_{\mathfrak{p}} \mathfrak{Z}(p^\infty)$;

(v) *H_3 is an arbitrary reduced p-group such that $0 \leqq \mathfrak{R}(H_3) \leqq \mathfrak{p}$.*

PROOF OF NECESSITY. First of all we prove that

(6) $$\mathfrak{R}(p^k G) = \mathfrak{R}(p^k H) \qquad \text{for } k = 0, 1, 2, \ldots .$$

Indeed, since H is a homomorphic image of G, we have $\mathfrak{R}(p^k G) \geqq \mathfrak{R}(p^k H)$ and, since G is isomorphic to some subgroup of H, we must also have $\mathfrak{R}(p^k G) \leqq \mathfrak{R}(p^k H)$.

Now apply Lemma 1 to get

$$G = G_1 + G' \quad \text{and} \quad H = H_1 + H'$$

where G_1 and H_1 are bounded groups, $p^m G_1 = p^m H_1 = 0$, plainly of power $\mathfrak{q}$, and G', H' are regular groups of power $\mathfrak{p}$. (If $\mathfrak{p} = \mathfrak{q}$, we set $G_1 = H_1 = 0$.) (6) implies $\mathfrak{R}(p^k G_1) = \mathfrak{R}(p^k H_1)$ $(k = 0, 1, \ldots, m-1)$ whence (i) holds, indeed.

Next we decompose G' and H' in the form

$$G' = G_2 + G_3, \qquad H' = H_2 + H_3$$

where G_2 and H_2 denote the maximal complete subgroup of G resp. H, and G_3, H_3 are reduced groups. Statement (ii) is evident in view of the definition of $\mathfrak{p}$. In order to establish (iv), let us take a basic subgroup B of G' satisfying the condition of Lemma 4. Then H, and hence H', contains a subgroup isomorphic to $G'/B \cong \sum\limits_{\mathfrak{p}} \mathfrak{Z}(p^\infty)$, and since $\mathfrak{R}_{p^\infty}(H) = \mathfrak{p}$, (iv) follows at once. (v) needs no detailed verification.

In order to establish (iii), we have only to prove that the first Ulm factor of G_3 has Property $A_\mathfrak{p}$ whence it will also follow that $|G_3| = \mathfrak{p}$ and G_3 is a regular group. First we observe that H_2, and hence H itself, contains a subgroup isomorphic to $A_\mathfrak{p}$ in (1). By hypothesis, G must have a factorgroup G/F isomorphic to $A_\mathfrak{p}$. In view of the fact that the property of being of infinite height is invariant under homomorphic mappings, we infer $G_2 \subseteq F$ as well as $G_3^* \subseteq F$ where G_3^* denotes the subgroup of G_3 consisting of all elements of infinite height in G_3 whence $\bar{G}_3 = G_3/G_3^*$ is the first Ulm factor of G_3. Therefore, $A_\mathfrak{p}$ is a homomorphic image of $G_1 + \bar{G}_3$ too, i. e. $(G_1 + \bar{G}_3)/C \simeq A_\mathfrak{p}$ for some subgroup C of $G_1 + \bar{G}_3$. If $G_1 = 0$, we are ready. If not, we observe that the last isomorphism implies that the factorgroup

$$(G_1 + G_3)/p^m C \simeq G_1 + (\bar{G}_3/p^m C)$$

may be mapped homomorphically upon $A_\mathfrak{p}$. Under this homomorphism $p^m[G_1 + (\bar{G}_3/p^m C)] = p^m(\bar{G}_3/p^m C)$ is mapped upon $p^m A_\mathfrak{p} \simeq A_\mathfrak{p}$. Hence we conclude that under the same homomorphism the image of $\bar{G}_3/p^m C$ has the property that if we multiply it by p^m, then we get a direct sum of cyclic groups. By a former result[15] we hence conclude that the image of $\bar{G}_3/p^m C$ is also a direct sum of cyclic groups, moreover, it follows at once that in this direct sum the set of the cyclic direct summands of order $\geqq p^k$ has the power $\mathfrak{p}$ for each natural k. This leads us to the conclusion that $\bar{G}_3$ has a homomorphic image isomorphic to $A_\mathfrak{p}$, that is, (iii) holds, in fact.

Proof of sufficiency. Let the p-groups G and H satisfy the conditions (i)—(v). The case $\mathfrak{p} = \mathfrak{q}$ (when $G_1 = H_1 = 0$) may easily be settled by observing that all p-groups of power $\leqq \mathfrak{p}$ (but no other groups) are subgroups of H (moreover of H_2) and the same groups (and no other ones) are homomorphic images of $A_\mathfrak{p}$ in (1) and hence (of G_3 and) of G.

Turning our attention to the case $\mathfrak{p} < \mathfrak{q}$, let us first note that if F is a homomorphic image of G or a subgroup of H, then we clearly have

$$\mathfrak{R}(p^k F) \leqq \mathfrak{R}(p^k G) = \mathfrak{R}(p^k H) \qquad (k = 0, 1, \ldots). \tag{7}$$

Conversely, let F be a p-group satisfying (7). Then, as in Lemma 1, one may conclude that F may be decomposed into a direct sum $F = F_1 + F_2$ such that $p^m F_1 = 0$ and $|F_2| \leqq \mathfrak{p}$. G and H must have a factorgroup resp. a subgroup isomorphic to F, for on the one hand F_1 and F_2 are homomorphic images of G_1 and G_3, respectively, while on the other hand they may isomorphically be imbedded in H_1 and H_2, respectively.

This completes the proof of Theorem 1.

Theorem 1 at the same time characterizes all pairs of F—S-dual torsion groups, for plainly *the torsion groups G and H are F—S-dual if and only if each of their p_i-components G_i and H_i are F—S-dual.*

[15] Fuchs [3], Theorem 4: If $nG\,(n \neq 0)$ is the direct sum of cyclic groups, then the same is true for G.

§ 5. *F—S*-dual mixed groups

We note that if G and H are $F—S$-dual groups, then H obviously must contain a non-zero torsion subgroup, but G may be torsion free. For the sake of convenience we agree to include this possibility into the case of mixed groups with which we shall be concerned in the present section.

THEOREM 2. *For an abelian mixed (or torsion free) group G we put* $\mathfrak{R}_\infty(G)=\mathfrak{r}$, $\mathfrak{R}_{p_i}(G)=\mathfrak{q}_i$, $\mathfrak{R}_{p_i^\infty}(G)=\mathfrak{p}_i$, $\mathfrak{t}_i=\max(\mathfrak{r},\mathfrak{p}_i)$.

The mixed groups G and H are $F—S$-dual if and only if they are of the form

(I) *in case* $\mathfrak{r}<\aleph_0$:

(8) $$G=\sum_n \mathfrak{Z}(\infty)+\sum_i G_i,\qquad H=\sum_n \mathfrak{Z}(\infty)+\sum_i H_i$$

where n is an arbitrary natural integer and, for each prime p_i, the p_i-groups G_i and H_i are unbounded $F—S$-dual groups;

(II) *in case* $\mathfrak{r}\geqq\aleph_0$:

(9) $$G=G_1+G_2+G_3,\qquad H=H_1+H_2+H_3+H_4$$

where

(i) $G_1=\sum_{\mathfrak{r}}\mathfrak{Z}(\infty)$, *i. e. a free abelian group of rank* $\mathfrak{r}$;

(ii) $G_2=\sum_i^* \sum_{\mathfrak{q}_i}\mathfrak{Z}(p_i^{k_i})$ *with* $1\leqq k_i\leqq m_i<\infty$, *the asterisk indicating that the summation is extended only over those primes p_i for which $\mathfrak{q}_i$ satisfies the inequality* $\mathfrak{q}_i>\mathfrak{t}_i$;

(iii) *G_3 is of torsion free rank $\leqq\mathfrak{r}$ such that the p_i-components U_i of its torsion subgroup U satisfy: in case $\mathfrak{p}_i\leqq\mathfrak{r}$, U_i is arbitrary with $\mathfrak{R}(U_i)\leqq\mathfrak{r}$, and in case $\mathfrak{p}_i>\mathfrak{r}$, U_i is a regular and reduced group satisfying $\mathfrak{R}(U_i)=\mathfrak{p}_i$ whose first Ulm factor has Property $A_{\mathfrak{p}_i}$;*

(iv) $H_1=\sum_{\mathfrak{r}}\mathfrak{R}$, *i. e. a complete torsion free group of rank* $\mathfrak{r}$;

(v) $H_2=\sum_i\sum_{\mathfrak{t}_i}\mathfrak{Z}(p_i^\infty)$ *(a complete torsion group);*

(vi) *H_3 is a torsion group such that $\mathfrak{R}_{p_i}(p_i^k G_2)=\mathfrak{R}_{p_i}(p_i^k H_3)$ for $k=0,1,\ldots$;*

(vii) *H_4 is a reduced group such that $\mathfrak{R}_\infty(H_4)\leqq\mathfrak{r}$ and $\mathfrak{R}_{p_i}(H_4)\leqq\mathfrak{t}_i$.*

PROOF OF NECESSITY. We remark in advance that if G and H are $F—S$-dual mixed groups, then H must have the same torsion free rank $\mathfrak{r}$ as G. Indeed, this follows by the same inference as we have applied in § 4, (6).

We select in H a maximal independent system (h_τ) consisting of elements of infinite order; then

$$S=\{\ldots,h_\tau,\ldots\}=\sum_{\mathfrak{r}}\{h_\tau\}\simeq\sum_{\mathfrak{r}}\mathfrak{Z}(\infty).$$

By hypothesis, G has a factorgroup G/G' isomorphic to S. Let $g_\mathfrak{r}$ denote arbitrary elements of G which are mapped upon the generators $h_\mathfrak{r}$ of the cyclic direct summands $\{h_\mathfrak{r}\}$ under some fixed homomorphism $G \sim S$ with the kernel G'. As readily checked, one has the decomposition

$$G = G_1 + G' \quad \text{with} \quad G_1 = \sum_{\mathfrak{r}} \{g_\mathfrak{r}\} \simeq \sum_{\mathfrak{r}} \mathfrak{Z}(\infty).$$

We first consider the case when $\mathfrak{r}$ is finite, say, $\mathfrak{r} = n > 0$. Clearly, then G' must coincide with the torsion subgroup T of G.

Let W denote the torsion subgroup of H. Since by hypothesis $G \sim H$ holds, we must also have $G \sim H/W$. The factorgroup H/W is a torsion free group of rank n, therefore the kernel of the homomorphism $G \sim H/W$ contains T and, since G/T and H/W have the same finite rank, no element of infinite order may have an image of finite order under the homomorphism $G/T \sim H/W$. We hence conclude that the kernel in question is just T:

$$H/W \simeq G/T \simeq \sum_{n} \mathfrak{Z}(\infty)$$

whence

$$H = X + W \quad \text{where} \quad X \simeq \sum_{n} \mathfrak{Z}(\infty).$$

Next we show that the torsion subgroups T and W are F—S-dual. Let K be a homomorphic image of T and hence of G; then it is isomorphic to some subgroup of H and hence of W. Conversely, if K is some subgroup of W, then $X + K$ is a subgroup of H and thus a homomorphic image of G. Under a homomorphism $G \sim X + K$ the inverse image K^* of K is a torsion subgroup considering that such a homomorphism preserves the torsion free rank n. On the other hand, K^* obviously contains T, thus $K^* = T$. This establishes the F—S-duality of T and W.

Finally, no p_i-component of W (and hence of T) is bounded, for G has a homomorphic image isomorphic to $G_1/p^k G_1$ for each natural k. Hence the necessity of (8) is proved.

Turning our attention to the case $\mathfrak{r} \geqq \aleph_0$, we first take into consideration that G_1 is a free abelian group of rank $\mathfrak{r}$ and therefore all abelian groups of power $\leqq \mathfrak{r}$ are homomorphic images of G_1 (and of G); for example, $\sum_{\mathfrak{r}} \mathfrak{R}$ is also one. From the F—S-duality of G and H it follows that H has a subgroup H_1,

$$H_1 \simeq \sum_{\mathfrak{r}} \mathfrak{R}.$$

But such a group is, by a well-known theorem,[4] necessarily a direct summand of H:

$$H = H_1 + H'$$

where we may assume that H' contains no subgroup isomorphic to $\mathfrak{R}$. Hence (iv) is established.

Let H_2 denote the maximal complete subgroup of H'. By our last assumption, H_2 is a torsion group and therefore the direct sum of quasi-cyclic groups:

$$H_2 = \sum_i \sum_{\mathfrak{s}_i} \mathfrak{Z}(p_i^\infty);$$

here we must have $\mathfrak{s}_i \geqq \mathfrak{r}$ for each prime p_i, in view of the fact that G_1 has a factorgroup and thus H has a subgroup isomorphic to $\sum_{\mathfrak{r}} \mathfrak{Z}(p_i^\infty)$ for each prime p_i. H_2 being a direct summand of H', we obtain

$$H = H_1 + H_2 + H''.$$

In order to complete the proof of assertion (v), we have still to show that $\mathfrak{s}_i = \mathfrak{t}_i = \max(\mathfrak{r}, \mathfrak{p}_i)$. Evidently, $\mathfrak{s}_i \geqq \mathfrak{p}_i$ follows from the fact that the p_i-component T_i of the torsion subgroup T of G has by Lemma 4 a basic subgroup B_i such that $T_i/B_i \simeq \sum_{\mathfrak{p}_i} \mathfrak{Z}(p_i^\infty)$, and T_i/B_i (as a complete group) being a direct summand of G/B_i, G has a factorgroup and thus H contains a subgroup isomorphic to $\sum_{\mathfrak{p}_i} \mathfrak{Z}(p_i^\infty)$. The kernel of the homomorphism $G \sim \sum_{\mathfrak{s}_i} \mathfrak{Z}(p_i^\infty)$ necessarily contains the group K consisting of all elements of G whose (finite) orders are relatively prime to p_i. The homomorphism $G/K \sim \sum_{\mathfrak{s}_i} \mathfrak{Z}(p_i^\infty)$ implies $p_i^{m_i}(G/K) \sim \sum_{\mathfrak{s}_i} \mathfrak{Z}(p_i^\infty)$ and since the torsion subgroup of $p_i^{m_i}(G/K)$ is a p_i-group of power $\mathfrak{p}_i$ and the torsion free rank of the same group is $\mathfrak{r}$, we are led to the conclusion that $\mathfrak{s}_i > \mathfrak{t}_i$ is impossible. Thus (v) is true, indeed.

We next apply Lemma 3 to the group G' to obtain

$$G' = G_2 + G_3$$

where G_2 is a torsion group whose p_i-components are bounded and G_3 has the property that $\mathfrak{R}_{p_i}(G_3) \leqq \mathfrak{t}_i$. This property does not alter if we separate from G_2 those of its p_i-components for which $\mathfrak{R}_{p_i}(G_2) \leqq \mathfrak{t}_i$ and incorporate them into G_3. Moreover, we may also assume that $\mathfrak{R}_{p_i}(p_i^{m_i} G_2) = 0$ where m_i is the least integer satisfying $\mathfrak{R}_{p_i}(p_i^{m_i} G') = \mathfrak{R}_{p_i^\infty}(G')$. Then we see that G_2 becomes a group of the form (ii).

Applying again Lemma 3, by the same argument as before we get for the group H'' a representation

$$H'' = H_3 + H_4$$

where the torsion group H_3 has bounded p_i-components which vanish for those primes p_i for which $\mathfrak{q}_i \leqq \mathfrak{t}_i$. Moreover, it is easily seen that there is no loss of generality in assuming that H_3 satisfies (vi). Then H_4 fulfils (vii).

As regards assertion (iii), we first observe that no detailed discussion is necessary in case $\mathfrak{p}_i \leqq \mathfrak{r}$, for then U_i surely possesses the stated property. Therefore suppose $\mathfrak{p}_i > \mathfrak{r}$. H_2 has a subgroup isomorphic to $A_{\mathfrak{p}_i} = A_{\mathfrak{t}_i}$,

and so the $F-S$-duality of G and H ensures the existence of a subgroup X_i of G such that

$$G/X_i \cong A_{\mathfrak{p}_i}.$$

As $A_{\mathfrak{p}_i}$ is a p_i-group containing no elements of infinite height, therefore both of the groups[16]

$$G_2^{(i)} = \sum_{j \neq i}^{*} \sum_{\mathfrak{q}_j} \mathfrak{Z}(p_j^{k_j}), \qquad Q_i = \sum_{j \neq i} U_j + U_i^*$$

(here U_i^* denotes the subgroup of U_i consisting of all elements having infinite height) are contained in X_i. In other words, $A_{\mathfrak{p}_i}$ is a homomorphic image of the group

$$G_1 + G_2/G_2^{(i)} + G_3/Q_i.$$

In this direct sum the second component being a bounded p_i-group (or zero), the same inference as that used in the proof of Theorem 1 (at the end of the necessity part) leads us to the conclusion that also

$$\bar{G} = G_1 + G_3/Q_i$$

has Property $A_{\mathfrak{p}_i}$. Under a homomorphism $\bar{G} \sim A_{\mathfrak{p}_i}$, the torsion subgroup $\bar{T}$ of $\bar{G}$ is mapped upon some subgroup A_* of $A_{\mathfrak{p}_i}$. Taking into account that the torsion free rank of $\bar{G}$ is just $\mathfrak{r}$ which is now less than $\mathfrak{p}_i$, it follows that $\mathfrak{R}(p_i^k A_*) = \mathfrak{p}_i$ for $k = 0, 1, \ldots$. But A_* as a subgroup of $A_{\mathfrak{p}_i}$ is necessarily again the direct sum of cyclic groups[17] and therefore we obtain that $\bar{T}$ — which is plainly isomorphic to the first Ulm factor U_i/U_i^* of U_i — has Property $A_{\mathfrak{p}_i}$. Hence it also follows that U_i is a regular p_i-group.

PROOF OF SUFFICIENCY. At first we show that G and H in (8) are $F-S$-dual. Let F be a factorgroup of G; then $\mathfrak{R}_\infty(F) = r \leq n$, furthermore, the factorgroup F/V of F with respect to its torsion subgroup V is a homomorphic image of G and hence of G/T. Therefore, F/V is the direct sum of r infinite cyclic groups and we arrive at a representation

$$F \cong \sum_r \mathfrak{Z}(\infty) + V. \tag{10}$$

Here V is a homomorphic image not only of $\sum_{n-r} \mathfrak{Z}(\infty) + T$, but also of T, for the p_i-components T_i of T are by hypothesis unbounded p_i-groups having $F-S$-dual pairs. Thus V may be imbedded isomorphically in W, consequently, F is isomorphic to some subgroup of H.

[16] The sum with the asterisk in the definition of $G_1^{(i)}$ has the same meaning as in Theorem 2, (ii).

[17] KULIKOV [7] and also FUCHS [3]. — Let us observe here that in the formulation of Theorem 3 in [3] the notion of subdirect sum is to be understood as a subgroup of the *discrete* direct sum (the footnote explaining this terminology, differring from the usual one, was unfortunately omitted).

Conversely, let F be a subgroup of H. Taking into account that now $F/V = F/(W \cap F) \simeq \{F, W\}/W$ is isomorphic to some subgroup of H/W, we arrive again at (10). Since V ($V \subset W$) must be a homomorphic image of T, F is evidently isomorphic to a factorgroup of G.

Turning our attention to case (II), let us suppose that G and H in (9) satisfy (i)—(vii). Let first F be a factorgroup of G; then we necessarily have

$$\mathfrak{R}_{\infty}(F) \leqq \mathfrak{r} \quad \text{and} \quad \mathfrak{R}_{p_i}(p_i^k F) \leqq \max(\mathfrak{r}, \mathfrak{R}_{p_i}(p_i^k G)) \qquad (k = 0, 1, \ldots).$$

We denote by k_i the greatest non-negative integer k with $\mathfrak{R}_{p_i}(p_i^k F) > \mathfrak{t}_i$; obviously, $k_i \leqq m_i$. By Lemma 3 we get a decomposition

$$F = F' + F'' \tag{11}$$

where the p_i-components F_i' of $F' = \sum_i^* F_i'$ are bounded ($p_i^{k_i} F_i' = 0$) and $\mathfrak{R}_{p_i}(F'') \leqq \mathfrak{t}_i$. Then, evidently, F' must be isomorphic to some subgroup of H_3, and since, by Lemma 5, F'' is isomorphic to some subgroup of $H_1 + H_2$, we have proved that F may isomorphically be imbedded in H, indeed.

In order to prove the converse, assume F is a subgroup of H. Then, obviously,

$$\mathfrak{R}_{\infty}(F) \leqq \mathfrak{r} \quad \text{and} \quad \mathfrak{R}_{p_i}(p_i^k F) \leqq \mathfrak{R}_{p_i}(p_i^k H) \qquad (k = 0, 1, \ldots).$$

We may again represent F in the form (11) with the same conditions on F' and F''. Now F' must be a homomorphic image of G_2, it is therefore enough to show that F'' is a homomorphic image of $G_1 + G_3$. But — as readily seen — this will follow at once if we can show that

$$\sum_{\mathfrak{r}} \mathfrak{Z}(\infty) + \sum_i A_{\mathfrak{t}_i}(p_i)$$

is a homomorphic image of $G_1 + G_3$, or more simply,

$$M = \sum_{\mathfrak{p}_i > \mathfrak{r}}^* A_{\mathfrak{p}_i}(p_i)$$

is a homomorphic image of G_3. By hypothesis, for the U_i with $\mathfrak{p}_i > \mathfrak{r}$ there is a subgroup Q_i in U_i such that

$$U_i/Q_i \simeq A_{\mathfrak{p}_i}.$$

Obviously, U/Q is the torsion subgroup of the group G_3/Q where

$$Q = \sum_{\mathfrak{p}_i > \mathfrak{r}}^* Q_i + \sum_{\mathfrak{p}_j \leqq \mathfrak{r}} U_j,$$

and clearly $U/Q \simeq \sum_{\mathfrak{p}_i > \mathfrak{r}}^* A_{\mathfrak{p}_i}$. For the group G_3/Q, all conditions of Corollary to Lemma 2 are satisfied, consequently, there exists a direct decomposition

$$G_3/Q = X/Q + Y/Q$$

where X/Q is a torsion group and Y/Q is of power $\leqq \mathfrak{r}$. Thus X/Q is on

the one hand a homomorphic image of G_3/Q, and on the other hand (as a subgroup of U/Q) the direct sum of cyclic groups which must have, for obvious reasons, M as a homomorphic image.

This completes the proof of Theorem 2.

§ 6. Dual and selfdual groups

The preceding discussions make possible to settle the problem of determining all pairs of dual groups and all selfdual groups. The following lemma enables us to reduce this problem to the case of selfdual groups; this lemma has been proved in [5], but for the sake of completeness we reproduce here its very simple proof.

LEMMA 6. *Two arbitrary groups G and H are dual if and only if they are selfdual and their standard manifolds coincide.* [18]

It is plainly sufficient to verify that the duality of G and H implies $S(G)=S(H)$. But this is a trivial consequence of the fact that, as G is a factorgroup of itself, G (and therefore every subgroup of G) is isomorphic to some subgroup of H, and conversely. Q. e. d.

Let us now consider a selfdual p-group G; we set $\mathfrak{K}_p(G)=\mathfrak{q}$ and $\mathfrak{K}_{p^\infty}(G)=\mathfrak{p}$. Then, by Theorem 1, G must have the form $G=G_1+G_2+G_3$ where G_1 is a bounded group, $G_2=\sum_{\mathfrak{s}} \mathfrak{Z}(p^\infty)$ with $0\leqq\mathfrak{s}\leqq\mathfrak{p}$ and G_3 is a reduced group of power $\mathfrak{p}$ whose first Ulm factor has property $A_\mathfrak{p}$. But now G must also satisfy the conditions given for H in Theorem 1. Consequently, G_2 as the maximal complete subgroup of G fulfils (iv) whence $\mathfrak{s}=\mathfrak{p}$. Thus we are led to the next theorem whose sufficiency part is by Theorem 1 quite obvious:

THEOREM 3. *Let G be an abelian p-group with $\mathfrak{K}(G)=\mathfrak{q}$ and $\mathfrak{K}_{p^\infty}(G)=\mathfrak{p}$. G is selfdual if and only if it has the form*

$$G=G_1+G_2+G_3 \tag{12}$$

where

(i) *in case* $\mathfrak{p}=\mathfrak{q}$: $G_1=0$,

in case $\mathfrak{p}<\mathfrak{q}$: $G_1=\sum_{\mathfrak{q}} \mathfrak{Z}(p^k)$ $(1\leqq k\leqq m<\infty)$, *i. e. the direct sum of cyclic groups of bounded order, the power of the set of components being* $\mathfrak{q}$;

(ii) $G_2=\sum_{\mathfrak{p}} \mathfrak{Z}(p^\infty)$;

(iii) *G_3 is a reduced and regular p-group of power $\mathfrak{p}$ whose first Ulm factor is of Property $A_\mathfrak{p}$.*

[18] The standard manifold of a selfdual group G is the set $S(G)=F(G)$. (Cf. [5].)

Let us turn to the case of mixed selfdual groups. Let G be such a group and put $\mathfrak{R}_\infty(G)=\mathfrak{r}$, $\mathfrak{R}_{p_i}(G)=\mathfrak{q}_i$, $\mathfrak{R}_{p_i^\infty}(G)=\mathfrak{p}_i$.

If $\mathfrak{r}=n$ is finite, then Theorem 2, (I) implies that G must have the form (8) where now evidently the p_i-groups G_i and H_i are unbounded and dual to each other.

If $\mathfrak{r}$ is infinite, then, by Theorem 2, (II), G is of the form $G=G_1+G_2+G_3^*$ where G_1, G_2 and G_3^* satisfy (i), (ii) and (iii), respectively. Theorem 2 also implies that G necessarily contains subgroups G_3 and G_4 isomorphic to H_1 and H_2 given by (iv) and (v), respectively. Considering that G_3+G_4 is a complete group and G_1+G_2 is reduced, we infer that G_3+G_4 is a subgroup and hence a direct summand of $G_3^*, G_3^*=G_3+G_4+G_5$. This also implies $\mathfrak{t}_i=\mathfrak{p}_i$, that is to say, $\mathfrak{p}_i\geqq\mathfrak{r}$. Now take into account that condition (iii) on G_3^* implies that G_5 has to satisfy (iii). This establishes the necessity of the condition contained in

THEOREM 4. *Suppose G is a mixed group with $\mathfrak{R}_\infty(G)=\mathfrak{r}$, $\mathfrak{R}_{p_i}(G)=\mathfrak{q}_i$, $\mathfrak{R}_{p_i^\infty}(G)=\mathfrak{p}_i$. G is selfdual if and only if it is of the form:*

(I) *in case* $\mathfrak{r}<\aleph_0$:

$$G=\sum_n \mathfrak{Z}(\infty)+\sum_i G_i \tag{13}$$

where G_i is an arbitrary selfdual unbounded p_i-group (covered by Theorem 3) and n is an arbitrary natural integer;

(II) *in case* $\mathfrak{r}\geqq\aleph_0$:

$$G=G_1+G_2+G_3+G_4+G_5 \tag{14}$$

where

(i) $G_1=\sum_{\mathfrak{r}}\mathfrak{Z}(\infty)$, *i. e. a free abelian group of rank* $\mathfrak{r}$;

(ii) $G_2=\sum_i^*\sum_{\mathfrak{q}_i}\mathfrak{Z}(p_i^k)$ *(with $1\leqq k\leqq m_i<\infty$), the asterisk indicating that the summation is extended only over those primes p_i for which $\mathfrak{q}_i$ satisfies the inequality* $\mathfrak{q}_i>\mathfrak{p}_i$;

(iii) $G_3=\sum_{\mathfrak{r}}\mathfrak{R}$, *i. e. a complete torsion free group of rank* $\mathfrak{r}$;

(iv) $\mathfrak{p}_i\geqq\mathfrak{r}$ *holds for each i and* $G_4=\sum_i\sum_{\mathfrak{p}_i}\mathfrak{Z}(p_i^\infty)$;

(v) *G_5 is of torsion free rank $\leqq\mathfrak{r}$ so that each p_i-component U_i of its torsion subgroup U satisfies: in case $\mathfrak{p}_i=\mathfrak{r}$ it is arbitrary with $\mathfrak{R}(U_i)\leqq\mathfrak{r}$, and in case $\mathfrak{p}_i>\mathfrak{r}$, U_i is a regular and reduced group of power $\mathfrak{p}_i$ whose first Ulm factor has Property $A_{\mathfrak{p}_i}$.*

The sufficiency of the stated condition is an immediate consequence of Theorem 2, because G has all the properties of the groups G and H in that theorem.

Our final result characterizes all pairs of dual groups. In view of Lemma 6, from Theorems 3 and 4 we obtain:

THEOREM 5. *The abelian groups G and H are dual if and only if they are selfdual and their corresponding invariants coincide.*

As a matter of fact, selfdual groups with the same invariants have the same form (12), (13) or (14), implying duality. The converse is trivial.

(Received 15 August 1953)

Bibliography

1. R. BAER, The subgroup of elements of finite order of an abelian group, *Annals of Math. (Princeton)*, (2), **37** (1936), pp. 766—781.
2. S. FOMIN, Über periodische Untergruppen der unendlichen Abelschen Gruppen, Матем. Сборник, **44** (1937), pp. 1007—1010.
3. L. FUCHS, The direct sum of cyclic groups, *Acta Math. Acad. Sci. Hung.*, **3** (1952), pp. 177—195.
4. L. FUCHS, On the structure of abelian *p*-groups, *Acta Math. Acad. Sci. Hung.*, **4** (1953), pp. 267—288.
5. L. FUCHS, A. KERTÉSZ and T. SZELE, On a special kind of duality in group theory. I, *Acta Math. Acad. Sci. Hung.*, **4** (1953), pp. 169—178.
6. Л. Я. Куликов, К теории абелевых групп произвольной мощности, Матем. Сборник, **9** (51) (1941), pp. 165—181.
7. Л. Я. Куликов, К теории абелевых групп произвольной мощности, Матем. Сборник, **16** (58) (1945), pp. 129—162.
8. Л. Я. Куликов, Обобщенные примарные группы. I, Труды Моск. Матем. Общ., **1** (1952), pp. 247—326.
9. А. Г. Курош, Теория групп (Москва, 1953), 2nd ed.
10. H. PRÜFER, Untersuchungen über die Zerlegbarkeit der abzählbaren primären Abelschen Gruppen, *Math. Zeitschrift*, **17** (1923), pp. 35—61.
11. T. SZELE, Ein Analogon der Körpertheorie für Abelsche Gruppen, *Journ. f. reine u. angew. Math.*, **188** (1950), pp. 167—192.
12. T. SZELE, On non-countable abelian *p*-groups, *Publicationes Math. (Debrecen)*, **2** (1952), pp. 300—301.
13. H. ULM, Zur Theorie der abzählbar-unendlichen Abelschen Gruppen, *Math. Annalen*, **107** (1933), pp. 774—803.

ОБ ОДНОМ СПЕЦИАЛЬНОМ ВИДЕ ДВОЙСТВЕННОСТИ В ТЕОРИИ ГРУПП. II

Л. ФУКС (Будапешт)

(Резюме)

В первой статье этого же заглавия Т. Селе, А. Кертес и автор настоящей статьи рассматривали и решили для случая счетных абелевых групп ряд вопросов, связанных с одной проблемой двойственности в теории групп. В настоящей работе эти результаты обобщены для случая абелевых групп произвольной мощности.

EINE BEMERKUNG ÜBER DIE CHARAKTERISIERUNG DER „KLASSISCHEN" ORTHOGONALEN POLYNOME

Von

J. ACZÉL (Debrecen)

(*Vorgelegt von* P. TURÁN)

1. Es sind zahlreiche Untersuchungen bekannt, die Eigenschaften angeben, die für die sog. klassischen, d. h. die Jacobischen, Laguerreschen und Hermiteschen Polynome gleichzeitig charakteristisch sind (vgl. [19]).

Z. B. wurde gefunden, daß nur diese solche Ketten orthogonaler Polynome bilden, deren Ableitungen wieder ein System von orthogonalen Polynomen geben ([9], [11], [12], [13], [15], [16], [22], [24]). Auch die besondere Gestalt der erzeugenden Funktion ([9], [10]) und der Rodriguesschen Formel ([8], [9]) wurde zur Charakterisierung herbeigezogen, obzwar auch für andere Systeme orthogonaler Polynome erzeugende Funktionen bzw. Rodriguessche Formeln angegeben werden können ([8], [9], [10]).

Die Polynome, die eine homogene lineare Differentialgleichung zweiter Ordnung erfüllen, wo der Koeffizient der Funktion selbst noch von n (dem Grade des Polynoms) abhängt, werden in mehreren Arbeiten ([3], [9], [23], [24]) angegeben. Diese Bedingung wird außer den klassischen noch von einer Anzahl anderer Polynomensysteme erfüllt, und, insbesondere wenn man auch die Abhängigkeit der übrigen Koeffizienten von n erlaubt, so geht die so charakterisierte Klasse von Polynomen weit über die klassischen hinaus ([1], [4], [9], [18]). In diesem Zusammenhang könnte es wohl nicht allzu schwer sein, die folgende Vermutung zu beweisen: die klassischen sind die einzigen solchen *Orthogonal*polynome, die Differentialgleichungen zweiter Ordnung des Sturm—Liouvilleschen Typs genügen.

Eine große Anzahl von Arbeiten enthält andererseits Beweise, daß die sog. Pearsonsche Differentialgleichung

$$\frac{p'(x)}{p(x)}=\frac{L(x)}{Q(x)}$$

(wo $L(x)$ bzw. $Q(x)$ Polynome von höchstens erstem bzw. zweitem Grade sind) mit Randbedingungen z. B.

$$\lim_{x\to a+0} Q(x)p(x)=\lim_{x\to b-0} Q(x)p(x)=0$$

oder mit Voraussetzung der Endlichkeit aller Momente von $p(x)$, die Gewichtsfunktionen $p(x)$ der klassischen orthogonalen Polynome vollständig bestimmt ([5], [6], [7], [14], [17], [20], [21]). Auch hier entstehen übrigens auch andere Arten orthogonaler Polynome, falls die allgemeinere Pearsonsche Differentialgleichung postuliert wird ([2]).

Der Verfasser der vorliegenden Arbeit hat sich — noch ohne Kenntnis der obenstehenden Resultate — das Ziel gesetzt, die klassischen Polynome und *nur diese*, durch *natürlich erscheinende* und in der Entwicklung der Theorie dieser Polynome auch sonst benutzte Eigenschaften (z. B. Rodriguessche Formel, Differentialgleichung, Orthogonalität) zu charakterisieren.

Das Resultat dieser Untersuchungen ist in der folgenden kleinen methodologischen Bemerkung enthalten, die auch für Unterrichtszwecke geeignet zu sein scheint.

2. Ein oft verfolgter Weg zur Behandlung der Jacobischen, Laguerreschen und Hermiteschen Polynome ist der folgende (z. B. [25]):

Man definiert die Folge von Polynomen $R_n(x)$ durch eine Rodriguessche Formel der Gestalt:

R) $$R_n(x) = \frac{u_n^{(n)}(x)}{p(x)}.$$

Hieraus erhält man die Differentialgleichung dieser Polynome, indem aus dem Zusammenhang der spezialen Gestalt der Funktion $u_n(x)$ mit der ihrer Derivierten das Bestehen einer Gleichung

$$Q(x)u_n'(x) = L_n(x)u_n(x)$$

folgt, woraus durch $(n+1)$-malige Derivation eine lineare Differentialgleichung $(n+2)$-ter Ordnung für $u_n(x)$ entspringt. Laut der Leibnizschen Regel für die n-te Derivierte eines Produktes enthält diese Gleichung dann und nur dann die Derivierten $u^{(n+2)}, u^{(n+1)}, u^{(n)}$ und nur diese, d. h. wir erhalten (vgl. R)) eine (homogen lineare) Differentialgleichung zweiter Ordnung für $R_n(x)$ genau dann, falls $L_n(x)$ bzw. $Q(x)$ Polynome höchstens von erstem bzw. zweitem Grade sind. Also soll in

D) $$Q(x)u_n'(x) = L_n(x)u_n(x)$$

$Q(x)$ höchstens *quadratisch*, $L_n(x)$ *linear* sein. — (Dies ist wieder die Pearsonsche Differentialgleichung, der aber hier $u_n(x)$ genügen muß.)

Endlich wird die Orthogonalität dieser Polynome durch n-malige partielle Integration in

$$\int_a^b p(x)R_n(x)R_m(x)\,dx = \int_a^b u_n^{(n)}(x)R_m(x)\,dx \qquad (m<n)$$

gezeigt (a und b sind endliche oder unendliche reelle Integrationsgrenzen).

Dies erfordert, daß die ausintegrierten Teile des Ausdruckes verschwinden, da dann

$$\int_a^b p(x)\, R_n(x)\, R_m(x)\, dx = (-1)^n \int_a^b u_n(x) R_m^{(n)}(x)\, dx = 0 \qquad (m < n)$$

wird. Dies ist dadurch gesichert, daß

O) *die Funktionen $u_n(x)$ in den zwei verschiedenen (endlichen oder unendlichen) reellen Punkten $x = a$ und $x = b$ Nullstellen n-ter Ordnung besitzen* ($n = 1, 2, \ldots$), undzwar, falls etwa $b = \infty$ ist, so muß $\lim_{x \to \infty} u_n(x) x^k = 0$ für jedes $k > 0$ gelten.

Hieraus ersieht man gleich, daß $p(x)$ die Gewichtsfunktion und (a, b) das Orthogonalitätsintervall unserer Polynome darstellt.

Im folgenden wollen wir zeigen, daß die klassischen Polynome vollständig charakterisiert werden durch die Bedingungen R), D) und eine weniger strenge Form N) der Bedingung O), in der nur die Existenz zweier gemeinsamen endlichen oder unendlichen reellen (wenigstens) einfachen Nullstellen a, b von $u_n(x)$ für jedes $n \geqq 1$ gefordert wird.

3. Wir beweisen also den folgenden

Satz. *Genügt eine Folge von Funktionen $u_n(x)$ der Differentialgleichung*

D) $$Q_n(x) u_n'(x) = L_n(x) u_n(x),$$

wo $L_n(x)$ bzw. $Q_n(x)$ Polynome von höchstens erstem bzw. zweitem Grade sind, und gilt:

N) *alle $u_n(x)$ $(n \geqq 1)$ besitzen wenigstens zwei verschiedene endliche oder unendliche reelle Nullstellen a, b gemeinsam,*

gibt es ferner eine Funktion $p(x)$ derart, daß für jedes n

R) $$\frac{u_n^{(n)}(x)}{p(x)} = R_n(x)$$

ein Polynom von genau n-tem Grade ist,

— dann ist $\{R_n\}$ eines der drei klassischen Systeme orthogonaler Polynome, nämlich das Jacobische bzw. Laguerresche bzw. Hermitesche, je nachdem die Polynome $Q_n(x)$ von zweitem bzw. erstem bzw. nulltem Grade sind.

Die Gewichtsfunktion der orthogonalen Polynome R_n wird $p(x)$ sein und ihr Orthogonalitätsintervall fällt mit dem Intervall $[a, b]$ der Nullstellen der Funktionen $u_n(x)$ zusammen.

Beweis. Wir lösen die Pearsonsche Differentialgleichung D):

$$\frac{u_n'(x)}{u_n(x)} = \frac{L_n(x)}{Q_n(x)}, \quad u_n(x) = \exp\left(\int \frac{L_n(x)}{Q_n(x)}\, dx\right).$$

Jetzt unterscheiden wir drei Fälle, je nachdem

1) $Q_n(x)$ von genau zweitem Grade ist,

2) $Q_n(x)$ linear ist,

3) $Q_n(x)$ konstant ist.

Hätte $Q_n(x)$ im Falle 1) keine oder nur eine (doppelte) reelle Wurzel, so wäre die Bedingung N) — wie man leicht einsieht — nicht erfüllt. Hat dagegen $Q_n(x)$ zwei verschiedene reelle Wurzeln a_n, b_n, so kann man schreiben:

$$\frac{L_n(x)}{Q_n(x)}=\frac{\alpha_n}{x-a_n}+\frac{\beta_n}{x-b_n}=\frac{\alpha_n}{x-a_n}-\frac{\beta_n}{b_n-x},$$

$$\int\frac{L_n(x)}{Q_n(x)}dx=\alpha_n\ln(x-a_n)+\beta_n\ln(b_n-x)+c_n,$$

$$u_n(x)=C_n(x-a_n)^{\alpha_n}(b_n-x)^{\beta_n}.$$

Wegen N) gilt, wie man gleich sieht, $\alpha_n>0$, $\beta_n>0$ $(n\geqq 1)$ und die a_n, b_n sind unabhängig von n:

$$u_n(x)=C_n(x-a)^{\alpha_n}(b-x)^{\beta_n}.$$

Da aber laut R) $(n=0)$

$$\frac{u_0(x)}{p(x)}=R_0=\text{konstant}$$

sein soll, wird

$$p(x)=\frac{C_0}{R_0}(x-a)^{\alpha}(b-x)^{\beta}$$

sein mit den verkürzten Bezeichnungen

$$\alpha_0=\alpha,\ \beta_0=\beta.$$

Dann muß aber wieder wegen R) für jedes n

$$K_n\frac{[(x-a)^{\alpha_n}(b-x)^{\beta_n}]^{(n)}}{(x-a)^{\alpha}(b-x)^{\beta}}=R_n(x)\qquad\left(K_n=\frac{C_nR_0}{C_0}\right)$$

eine ganze rationale Funktion n-ten Grades sein, was nur dann eintrifft, wenn für jedes n

$$\alpha_n=\alpha+n,\quad \beta_n=\beta+n$$

ist.

(Es kann nämlich

$$(x-a)^{-\alpha}(b-x)^{-\beta}[(x-a)^{\alpha_n}(b-x)^{\beta_n}]^{(n)}=$$
$$=(x-a)^{\alpha_n-n-\alpha}(b-x)^{\beta_n-n-\beta}[c_0(x-a)^n+(x-a)(b-x)P_{n-2}(x)+c_n(b-x)^n]$$

nur dann ein Polynom n-ten Grades sein, falls einerseits $\alpha_n+\beta_n-\alpha-\beta=2n$, anderseits $\alpha_n-n-\alpha\geqq 0$, $\beta_n-n-\beta\geqq 0$ ist, woraus $\alpha_n=\alpha+n$, $\beta_n=\beta+n$ folgt.)

Das heißt: die Polynome

$$R_n(x)=K_n(x-a)^{-\alpha}(b-x)^{-\beta}[(x-a)^{\alpha+n}(b-x)^{\beta+n}]^{(n)}=\bar{J}_n^{(\alpha,\beta)}(x)$$
$$(\alpha>-1,\beta>-1)$$

sind bis auf eine lineare Transformation mit den *Jacobischen Polynomen* identisch. Die Gewichtsfunktion ist hier $(x-a)^{\alpha}(b-x)^{\beta}$, das Orthogonalitätsintervall ist $[a,b]$.

Im Falle 2) wird ebenso:

$$\frac{L_n(x)}{Q_n(x)} = A_n + \frac{\alpha_n}{x-a_n},$$

$$\int \frac{L_n(x)}{Q_n(x)} dx = A_n x + \alpha_n \ln (x-a_n) + c_n,$$

$$u_n(x) = C_n (x-a_n)^{\alpha_n} e^{A_n x} = C_n (x-a)^{\alpha_n} e^{A_n x} \qquad (a_n \equiv a,\ A_n \neq 0),$$

$$p(x) = \frac{u_0(x)}{R_0} = \frac{C_0}{R_0}(x-a)^\alpha e^{Ax} \qquad (\alpha_0 = \alpha,\ A_0 = A),$$

$$K_n \frac{[(x-a)^{\alpha_n} e^{A_n x}]^{(n)}}{(x-a)^\alpha e^{Ax}} = R_n(x) \qquad \left(K_n = \frac{C_n R_0}{C_0}\right)$$

$$A_n \equiv A,\ \alpha_n = \alpha + n,$$

$$R_n(x) = K_n (x-a)^{-\alpha} e^{-Ax} [(x-a)^{n+\alpha} e^{Ax}]^{(n)} = \overline{L}_n^{(\alpha)}(x) \qquad (\alpha > -1)$$

und dies sind eben die linearen Transformierten der *allgemeinen Laguerreschen Polynome* mit der Gewichtsfunktion $(x-a)^\alpha e^{Ax}$ und dem Orthogonalitätsintervall $[a, \infty)$ bzw. $(-\infty, a]$, je nachdem $A \lessgtr 0$ ist.

Endlich kann im Falle 3)

$$\frac{L_n(x)}{Q_n(x)} = -2A_n(x-B_n),$$

$$\int \frac{L_n(x)}{Q_n(x)} dx = -A_n(x-B_n)^2 + c_n,$$

$$u_n(x) = C_n e^{-A_n(x-B_n)^2}$$

geschrieben werden, wo

$$A_n > 0$$

sein muß, da sonst $u_n(x)$ entgegen N) überhaupt keine, weder endliche, noch unendliche Nullstellen besitzt. Aus R) folgt wieder

$$p(x) = \frac{C_0}{R_0} e^{-A(x-B)^2} \qquad (A_0 = A,\ B_0 = B),$$

$$A_n \equiv A, \quad B_n \equiv B,$$

$$R_n(x) = K_n e^{A(x-B)^2} [e^{-A(x-B)^2}]^{(n)} = \overline{H}_n(x).$$

Dieser Fall ergibt also die (linear transformierten) *Hermiteschen Polynome* mit der Gewichtsfunktion $e^{-A(x-B)^2}$ und dem Orthogonalitätsintervall $(-\infty, \infty)$.

Hiermit ist also der Beweis vollendet.

Man bemerkt, daß N) nur zur Absonderung von drei Funktionentypen (komplexe oder zusammenfallende Wurzeln in 1), negatives A in 3)), sowie zur Begründung der Beschränkungen $\alpha > -1$, $\beta > -1$ benutzt wurde.

Verglichen mit der üblichen Behandlungsweise, die die Gültigkeit der Pearsonschen Differentialgleichung für $p(x)$ fordert (vgl. 1.), sind unsere Forderungen stärker, dagegen scheinen sie mehr natürlich zu sein, als die dort geforderten Bedingungen.

(Eingegangen am 2. November 1953.)

Literaturverzeichnis

[1] T. J. Stieltjes, *Oeuvres completes* (Groningen, 1914), S. 432—439.

[2] V. Romanovski, Sur quelques classes nouvelles des polynomes orthogonaux, *Comptes Rendus Acad. Sci., Paris,* **188** (1929), S. 1023—1025.

[3] S. Bochner, Über Sturm—Liouville Polynomsysteme, *Math. Zeitschr.*, **29** (1929), S. 720—736.

[4] J. Chokhate (Shohat), Sur une classe étendue de fractions continues algébriques et sur les polynomes de Tchebycheff correspondents, *Comptes Rendus Acad. Sci., Paris,* **191** (1930), S. 989—990.

[5] E. H. Hildebrandt, Systems of polynomials connected with the Pearson differential and difference equations, *Bulletin Amer. Math. Soc.*, **37** (1931), S. 676.

[6] E. H. Hildebrandt, Systems of polynomials connected with the Charlier expansions and the Pearson differential and difference equation, *Annals of Math. Stat.*, **2** (1931), S. 379—439.

[7] M. Marden, A rule of signs involving certain orthogonal polynomials, *Annals of Math.*, **33** (1932), S. 118—124.

[8] N. Abramesco, Les polynomes orthogonaux, *Annales Fac. Sci. Univ. Toulouse*, (3), **24** (1932), S. 67—87.

[9] J. Shohat (Chokhate), Théorie générale des polynomes orthogonaux de Tchebycheff, *Mémorial des Sci. Math.*, **66** (Paris, 1934), insb. S. 15—18 und S. 31—36.

[10] J. Meixner, Orthogonale Polynomsysteme mit einer besonderen Gestalt der erzeugenden Funktion, *Journal London Math. Soc.*, **9** (1934), S. 6—13.

[11] W. Hahn, Über die Jacobischen Polynome und zwei verwandte Polynomklassen, *Math. Zeitschr.*, **39** (1935), S. 634—638.

[12] H. L. Krall, On derivatives of orthogonal polynomials, *Bulletin Amer. Math. Soc.*, **42** (1936), S. 423—428.

[13] H. L. Krall, On higher derivatives of orthogonal polynomials, *Bulletin Amer. Math. Soc.*, **42** (1936), S. 867—870.

[14] S. Koulik, Les polynomes orthogonaux en connection avec certaines schémes de distributions discrétes de probabilités, *J. Inst. Math. Acad. Sci. Ukraine*, **1** (1937), S. 89—136.

[15] M. S. Webster, Orthogonal polynomials with orthogonal derivatives, *Bulletin Amer. Math. Soc.*, **44** (1938), S. 880—888.

[16] W. Hahn, Über höhere Ableitungen von Orthogonalpolynomen, *Math. Zeitschr.*, **43** (1938), S. 101.

[17] C. E. Dieulefait, Die Momente einer Gruppe von Wahrscheinlichkeitsfunktionen und ihre Beziehungen zu den linearen Differentialgleichungen zweiter Ordnung, den Gleichungen von Laplace, den algebraischen Kettenbrüchen und den Summen divergenter Reihen, *An. Soc. Ci. Argentina*, **125** (1938), S. 81—111.

[18] J. Shohat, A differential equation for orthogonal polynomials, *Duke Math. Journal*, **5** (1939), S. 401—417.

[19] J. Shohat, E. Hille, J. L. Walsh, A Bibliography on orthogonal polynomials, *Bull. of the Nat. Res. Council*, **103** (Washington, 1940).

[20] F. S. Beale, On a certain class of orthogonal polynomials, *Annals of Math. Stat.*, **12** (1941), S. 97—103.

[21] D. Jackson, *Fourier-series and orthogonal polynomials*, Carus Monograph 6 (Oberlin, Ohio, 1941), Ch. VI, VII. 10.

[22] H. L. Krall, On derivatives of orthogonal polynomials. II, *Bulletin Amer. Math. Soc.*, **47** (1941), S. 261—264.

[23] F. Simonart, Sur les systémes de polynomes de Sturm—Liouville, *Acad. Roy. Belg., Cl. Sci.*, (5), **33** (1947), S. 8—21.

[24] W. Hahn, Über Orthogonalpolynome, die q-Differenzengleichungen genügen, *Math. Nachrichten*, **2** (1949), S. 4—34.

[25] И. П. Натансон, Конструктивная теория функций (Москва—Ленинград, 1949), §§ VI. 1, 2, VIII. 3, 4.

ЗАМЕЧАНИЕ К ХАРАКТЕРИЗОВАНИЮ КЛАССИЧЕСКИХ ОРТОГОНАЛЬНЫХ МНОГОЧЛЕНОВ

Я. АЦЕЛ (Дебрецен)

(Резюме)

В настоящей работе даются свойства характеризующие многочлены Якоби, Лагерра и Эрмита, и только эти три классы многочленов. Эти свойства: ортогональность, существование однородного линейного дифференциального уравнения второго порядка, и формулы Родригеса.

Точнее говоря, эти полиномы допускают представление в виде частного n-ой производной некоторой функции $u_n(x)$ и весовой функции $p(x)$. $u_n(x)$ имеет для всякой $n>0$ две общие (конечные или бесконечные) корни, и она удовлетворяет однородному линейному дифференциальному уравнению первого порядка, первый коэффициент которого есть многочлен не выше второй степени, а второй коэффициент полином не выше первой степени.

Излагаются также другие относящиеся к этому кругу вопросов результаты, и формулируется гипотеза, что только эти три классы ортогональных полиномов удовлетворяют уравнению второго порядка типа Штурма—Лиувилля.

Technikai szerkesztő: Fuchs László

A kiadásért felelős: Mestyán János. Műszaki felelős: Tóth Ferenc
A kézirat beérkezett: 1953. VII. 13. — Példányszám: 800. — Terjedelem: 15¹ ₂ (A/5) ív, 12 ábra.

Csongrádmegyei Nyomdaipari Vállalat, Szeged 53 3050 Felelős vezető Vincze György

The Acta Mathematica publish papers on mathematics in English, German, French and Russian.

The Acta Mathematica appear in parts of various size, making up volumes.

Manuscripts should be adressed to:

Acta Mathematica, Budapest 502, Postafiók 24.

Correspondence with the editors and publishers should be sent to the same address

The rate of subs.cription to the Acta Mathematica is 110 forints a volume. Orders may be placed with „*Kultura*" Foreign Trade Company for Books and Newspapers (Budapest, I., Fő utca 32. Account No. 43-790-057-181) or with representatives abroad.

Les Acta Mathematica paraissent en français, allemand, anglais et russe et publient des mémoires du domaine des sciences mathématiques.

Les Acta Mathematica sont publiés sous forme de fascicules qui seront réunis en volumes

On est prié d'envoyer les manuscrits destinés à la rédaction à l'adresse suivante:

Acta Mathematica, Budapest 502, Postafiók 24.

Toute correspondance doit être envoyée à cette même adresse.

Le prix de l'abonnement est de 110 forints par volume.

On peut s'abonner à l'Entreprise pour le Commerce Extérieur de Livres et Journaux „*Kultura*" (Budapest, I, Fő utca 32. Compte-courant No. 43-790-057-181) ou à l'étrange chez tous les représentants ou dépositaires.

„*Acta Mathematica*" публикует трактаты из области математических наук на русском немецком, английском и французском языках.

„*Acta Mathematica*" выходит отдельными выпусками разного объема. Несколько выпусков составляют один том.

Предназначенные для публикации рукописи следует направлять по адресу:

Acta Mathematica, Budapest 502, Postafiók 24.

По этому же адресу направлять всякую корреспонденцию для редакции и администрации.

Подписная цена „*Acta Mathematica*" — 110 форинтов за том. Заказы принимает предприятие по внешней торговле книг и газет „*Kultura*" (*Budapest, I., Fő utca 32.* Текущий счет № 43-790-057-181) или его заграничные представительства и уполномоченные.

Reprinted by arrangement with the publishers
„KULTURA" Hungarian Trading Company
for Books and Newspapers
Budapest, POB. 149.
Hungary